CHECKLIST for
INTERNET PROTOCOL TELEPHONY VOICE OVER INTERNET PROTOCOL
V2R2.1

21 APRIL 2006

Developed by DISA for the DOD

Database Reference Number: ______________________________ CAT I: _____

Database entered by: _________________ Date: _____________ CAT II: _____

Technical Q/A by: ____________________Date: _____________ CAT III: _____

Final Q/A by: _______________________ Date: _____________ CAT IV: _____

Total: _____

UNCLASSIFIED UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Enclave Reviewer			**Phone**		
Previous SRR	Y N	**Date of Previous SRR**		**S01 Available**	Y N
Number of Current Open Findings					

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

PROCEDURES FOR REGISTRATION OF VOICE/VIDEO/RTS ASSETS IN THE VMS

1.1 Introduction

This document will describe the proper procedure to follow to register and update the IA status of voice and/or video / real time services (RTS) systems and devices in VMSv6. For the purpose of this document, we will use RTS to refer to any voice/video/RTS system or device. This includes all types of telecom switches or video systems, whether they are TDM or IP based, as well as any supporting system or device.

1.1.1 Pre - Requisites

Any person that needs to interface with the VMSv6 must:

1. Take the on-line CBT, which can be accessed at https://vmscbt.disa.mil (no login is required). It is highly recommended that a person taking the CBT review all modules to become familiar with all of the roles that the various VMS users fulfill.

2. Download and become familiar with the appropriate users guide for user role(s) that the trainee will be fulfilling. These bay be found at https://vmscbt.disa.mil/resources.htm
3. Obtain a VMS account and login to the application. Instructions for this are contained in the CBT.
4. Become familiar with the navigation and features of VMS by reviewing the CBT and users guide while in VMS.

Once these steps have been completed, one can begin to register assets and update their statuses.

1.2 RTS Asset Naming Convention

A naming convention for the system and its components must be used when registering the various assets so that the individual assets can be more easily identified as a group or part of a system. This naming convention should be based on the name of the owner/site/location/enclave and the name/type of RTS system being registered.

Some examples of an overall RTS system name might be:

- DISA-SKY7_Cisco-VoIP
- Ft.Hood_MSL100
- LacklandAFB_MSL100
- Gunter_CS2100
- Landstuhl_HiPath4000
- SHAPE_EWSD
- Pearl_5ESS

This name represents the Non-Computing Asset for the overall RTS system.

The Computing Assets, that make up the RTS system must include the name of the overall system and a unique name for the device. This unique name should include the function of the device and its network addressable name. That is the unique name that is used to identify the box on the network. This is not the IP address or MAC address, which is entered as an attribute of the asset.

Some examples of component device/system names might be:

- DISA-SKY7_Cisco-VoIP_CCM-Registrar_CCM0001RP
- DISA-SKY7_Cisco-VoIP_CCM-Publisher_CCM0002PP
- DISA-SKY7_Cisco-VoIP_CCM-B/URegistrar_CCM0003RB
- DISA-SKY7_Cisco-VoIP_CCM-B/UPublisher_CCM0004PB
- DISA-SKY7_Cisco-VoIP_PSTN-Gateway_PSTNGW0001
- DISA-SKY7_Cisco-VoIP_DSN-Gateway_DSNGW0001
- DISA-SKY7_Cisco-VoIP_LAN-Core_SKY70001
- DISA-SKY7_Cisco-VoIP_ManagementWS_SKY7MWS0001
- DISA-SKY7_Cisco-VoIP_ManagementLS_SKY7MLS0001

In the event that an asset already exists and uses a different naming convention, place the name derived here the asset ‘Description’ field.

1.3 RTS Asset Identification

An RTS system as a whole is an asset, however, each individual device that makes up the system is also an asset. Each of these assets must be registered in the VMS. VMS has 2 primary types of assets, Computing and Non-Computing.

Each RTS system at a given site/location/enclave needs to be registered as a Non-Computing Asset in the VMS.

The individual assets are registered as Computing Assets. Computing Assets are based on boxes, which have an operating system (OS) as well as applications such as databases, web servers, and control and/or management applications. The OS and the applications are called “Postures” in the VMS. All applicable postures are assigned to the asset.

Typically, a Computing Asset will have at least one IP address and/or one MAC address. Management workstations, LAN switches and routers, firewalls, multiplexers, phones, and similar devices are also Computing Assets that make up the RTS system. Desktops and Laptops are also computing devices that need to be registered.

1.3.1 Local Management System(s)

LAN switches and routers, management workstations/consoles, NMS servers, and front end processors that are used exclusively in the local management the RTS system must be named and registered as part of the RTS system and given a unique name (using the naming convention above) identifying it as part of the RTS system. Local management systems must be treated as an enclave.

1.3.2 Remote Management System(s)

LAN switches and routers, management workstations, NMS servers, and front end processors, etc that are part of a remote management/monitoring system such as ADIMSS, ARDIMSS, ESRS, etc, must be registered by the owner/SA of the device or the owner/SA of the management/monitoring system that it is part of. It is critical that the ‘Location’, ‘Managed By’, and ‘Owned by’ fields are properly filled out. The device or system must also be associated with the proper program(s), site, and enclave under the ‘Sites/Enclaves’ tab. Remote management systems are typically separate enclaves from the local management system enclaves.

1.3.3 BCPS LAN/CAN/BAN Infrastructure

LAN switches and routers that make up the data and RTS distribution system must be named and registered by the LAN/enclave SA in accordance with the Network Infrastructure asset registration instructions found in the Network Infrastructure Checklist. RTS requirements for the LAN are applied to the asset via the Non-Computing asset assignment of the RTS requirements to it as described below.

1.3.4 RTS Adjunct/Auxiliary Systems/Devices

Adjunct/Auxiliary Systems/Devices are defined as systems and devices that augment the basic telephony service. Examples of such systems and devices are: Voice mail systems, call center and/or operator systems, CTI systems, IVR systems, auto-attendant systems, Emergency Services (911) systems, etc. Systems such as these may be registered as part of the RTS system if appropriate (i.e., small systems or single devices), or may be registered as a separate Non-Computing system / enclave asset along with its Computing assets.

1.4 RTS Asset Creation In The VMS

The RTS system Non-Computing Asset(s) is(are) registered first, followed by the Computing Assets. This section will provide an overview of the major steps. Subsequent sections will provide step-by-step procedures.

1.4.1 The Organization, Site, and/or Location

Before assets can be created, an organization and a site or location must be defined in the VMS. This is a VMS ISSM role and responsibility and is outside the scope of this document. Programs are also defined in the VMS and this is the responsibility of the VMS DAA role.

1.5 Non-Computing Asset Creation

First create the Non-Computing Asset for the RTS system using the naming convention described in "RTS Asset Naming Convention" above. On the 'Asset Posture' tab, expand the 'Voice/Video/RTS Policy' item and check the policies that apply. The available policies are:

- DRSN Policy
- DSN Policy
- VoIP/VoSIP Policy

'DRSN Policy' applies to an asset that is part of, or connected to, the DRSN. This can also apply to other "secure" or classified voice/video/RTS systems.
'DSN Policy' applies to an asset that is part of, or connected to, the DSN. or other UN-classified voice/video/RTS systems.. All UN-classified voice/video/RTS systems owned or operated by, or for, the DoD are subject to the same requirements.
'VoIP/VoSIP Policy' applies to an asset being registered that provides IP based voice or video communications (i.e., VoIP). This includes IP centric systems as well as IP enabled TDM based systems.

Either DSN Policy **OR** DRSN Policy must be checked. VoIP/VoSIP Policy must **ALSO** be checked if the system provides IP based voice or video communications.

A local RTS system management LAN, that is not part of the site LAN, should be added to, or registered as part of, the RTS Non-Computing Asset. Additionally, a LAN that only supports an adjunct/auxiliary system to the RTS system, such as a call center or IVR system may be added to or registered as part of the RTS Non-Computing Asset.

This is done by adding the 'Network Infrastructure Policy' and/or the 'General Business LAN Enclave' postures.

Additionally, an adjunct/auxiliary system to the RTS system (and its supporting LAN) such as a call center or IVR system etc, that is not part of the site LAN, may be registered a separate complete system to include its supporting LAN. Such a system is registered as a Non-Computing Asset using the naming convention for the overall RTS system and adding the adjunct/auxiliary system name. For Example:

- LacklandAFB_MSL100_CallCtr-Sys
- LacklandAFB_MSL100_IVR-Sys
- LacklandAFB_MSL100_911-Sys

This is done by adding the ‘Network Infrastructure Policy’ and/or the ‘General Business LAN Enclave’ as well as the ‘Voice/Video/RTS Policy’ postures to the Non-Computing Asset.

The second Non-Computing Asset that needs registration consideration is the site LAN/CAN/BAN that provides distribution for both RTS services and data traffic. This network must be registered along with its components whether it supports RTS systems or not. The SA for the RTS system must work with the SA for the LAN/CAN/BAN to insure that the Voice/Video/RTS Policy asset postures are selected as described above for the RTS System itself. These two SAs could be the same person, however, if not, the SA for the LAN/CAN/BAN should grant “update” permissions on LAN assets to the SA for the RTS system. Asset naming would follow that chosen by the SA for the LAN/CAN/BAN.

Alternately, the SA for the RTS system could create his/her own LAN/CAN/BAN Non-Computing Asset and assign the ‘Voice/Video/RTS Policy’ asset postures to it. Asset naming would follow the naming convention described in “RTS Asset Naming Convention” above. In this case, the individual LAN/CAN/BAN Computing Assets would not be registered since the SA for the LAN/CAN/BAN would register these.

Detailed step-by-step process instructions are provided under “Creating the Non-Computing Asset(s)” below.

1.5.1 Computing Asset Creation

All system devices must be defined and registered once the appropriate NON-Computing Assets are created, and the BCPS LAN/CAN/BAN has had the Voice/Video/RTS Policies added to it. The SA for the BCPS LAN/CAN/BAN must register each LAN switch, router, and management system. This does not have to be done by the RTS system SA unless he/she is also the SA for the BCPS LAN/CAN/BAN, or if the RTS system SA has created a separate Non-Computing Asset for the RTS BCPS LAN/CAN/BAN.

The following are examples of RTS Computing Assets: (Note: Some of these may have sub-components that are also considered as individual Computing Assets.)

- TDM Switch (Possible sub-components)
- Local Call Controller (Possible sub-components)
- Call Manager Subscriber
- Call Manager Publisher
- Media gateway
- RTS firewall or Boundary control device

- LAN Switch / Router
- Phone instrument – endpoint
- Management workstation
- NMS data collection device or server
- Server (of almost any type)
- VTC MCU (Possible sub-components)
- VTC endpoint
- Gatekeeper
- All GSCR device type designations:
- Many others

All computing assets are registered with an OS. They may also have applications such as databases and/or web servers that also must be added to the posture of the asset.

Registering computing assets is an iterative process until all assets are registered.

Detailed step-by-step process instructions are provided under “Creating the Computing Asset(s)” below.

1.6 Creating Assets – Step-by-Step

1.6.1 Creating the NON-Computing Asset(s)

These instructions apply to creating the RTS system and/or Adjunct/Auxiliary system NON-Computing Asset.

Note: *(Reviewer)* It is recommended that a reviewer work with the Voice/Video/RTS system SA when creating assets for this type of system. The SA will have more knowledge of the system and can assist in making sure that all applicable postures are applied and that the system naming, identification, enclaves, and programs are selected or applied properly.

a. Steps

i. **Expand 'Asset Findings Maint'**

ii. **Click 'Assets/Findings'**

iii. **Expand 'By Location'** and then find and expand your site/location. (Others may need to expand 'Managed By' or 'Owned By'. What is seen depends upon your permissions or role.) Within the location, assets are divided into computing, non-computing and CNDS.
   - o Proceed to step vi.

   (Reviewer Only) Expand 'Visits' to display its sub-folders.

iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. **Click the 'yellow folder'** icon located at the right of 'Non-Computing'. You may expand 'Non-Computing' to see assets that have already been created and that you have permissions for.

vii. **Click the 'General' tab**
   - o Enter a 'Host Name' using the naming convention described in "RTS Asset Naming Convention" above.
   - o Enter a 'Description' of the system.
     Note: This should reflect a general description of the RTS System and could include the make and version of the LCC software.
   - o Verify/Select the location of the system in "Location"
   - o Verify/Select the owner of the system in "Owner": (Used to register asset to parent or child location.)
   - o Verify/Select the organization or site responsible for management of the system in "Managed By": (Used for remotely managed locations.)
   - o Verify 'Mac level', 'Confidentiality', & 'Classification', Change as required.
     Note: These default to MAC II, Sensitive, Unclassified. The 'Confidentiality' of a RTS system or asset should never be set to 'Public' since its configuration is considered sensitive. These settings should match those identified in the site or system SSAA.
   - o Click 'Save'.

Note: It is recommended that you click 'Save' after filling out each tab or more often. This practice will prevent the loss of recently entered data in the event of a timeout. You may wait to save until after filling out all tabs but you must click save at the end of data entry on all tabs or your work will be lost.

viii. **Click the 'Asset Posture' tab** to add functions to the asset:

- o Expand 'Non-Computing'
- o Expand 'Voice/Video/RTS Policy' (or 'Telecom Policy')
- o Check the boxes for appropriate policy/policies as follows:
  - Check 'DRSN Policy' if the asset is part of, or is connected to, the DRSN. **Note**: This policy can also apply to other "secure" or classified voice/video/RTS systems.

  OR

  - Check 'DSN Policy' if the asset is part of, or is connected to, the DSN. **Note**: This apples to ALL UN-classified voice/video/RTS systems whether part of the DSN or not. All UN-classified voice/video/RTS systems owned or operated by, or for, the DoD are subject to the same requirements.

  AND

  - Check 'VoIP/VoSIP Policy' if the system being registered provides IP based communications. This includes IP centric systems and IP enabled TDM based systems.

  AND

  - (Conditional) If there is a LAN that only supports the management of the RTS system or an adjunct/auxiliary system to the RTS system AND it is not part of the site LAN/CAN/BAN or the site's OOB management LAN:
    - o Expand 'Network Policy Requirements'
    - o Check 'Network Infrastructure Policy'

    Note: If such a LAN is not added here it must be registered separately under both Non-Computing and Computing. Adjunct/auxiliary systems LANs and devices may also be registered separately.

  AND

  - (Conditional) If this LAN has a boundary that touches another LAN, or a local / extended enclave, or a DoD WAN:
    - o Expand 'Enclave'
    - o Check 'General Business LAN Enclave'.
- o Click '>>' to move it to the 'Selected' window (This can be done after each selection or after all selections).
- o Click 'Save'

ix. **Click the 'Systems / Enclaves' tab** to associate this asset with the appropriate or all applicable program(s), enclave(s), and site(s).

- o Determine the enclave and/or program that the asset is part of.
- o In the 'Available Systems' box:
  - Find and select 'DISN-DSN' if the system can place or receive DSN calls.

  OR

  - Find and select 'DISN-DRSN' if the system can place or receive DRSN calls. (Not available as of 4/7/05 See note below)
  - Click '>>' to move it to the 'Selected Systems' window

- Click 'Save' (optional)

AND

- Find and select 'ADIMSS', IF the RTS System is managed or monitored by the ADIMSS (DSN),

OR

- IF the RTS System is managed or monitored by the ARDIMSS or ESRS (DRSN), Find and select 'ARDIMSS' and/or 'ESRS'
- Click '>>' to move it to the 'Selected Systems' window
- Click 'Save' (optional)

o In the 'Available Enclaves' box:

- Find and select the local enclave that the RTS system is part of. (i.e., your site/location)
- Click '>>' to move it to the 'Selected Enclaves' window
- Click 'Save'

Note: For registered enclaves and/or programs, choose all that apply. If the enclave or program is not present, ensure that the IAM [or *(Reviewer Only)* Team Lead] works with the appropriate site personnel to request the enclave or program be added.

x. **Click the 'Additional Details' tab** to add building and room number information for the RTS asset; this should reflect the location of the RTS core equipment.

xi. **Click 'Save'**.

xii. Return to step vi to create another Non-Computing asset or proceed to creating the Computing Assets in the next section.

Note: The above 'Voice/Video/RTS Policy' postures and program association may be added to an enclave or network non-computing asset instead of creating a separate Voice/Video/RTS non-computing asset.

1.6.2 Creating the Computing Assets

These instructions apply to creating the RTS system and/or Adjunct/Auxiliary system Computing Asset(s).

Note: *(Reviewer)* It is recommended that a reviewer work with the Voice/Video/RTS system SA when creating assets for this type of system. The SA will have more knowledge of the system and can assist in making sure that all applicable postures are applied and that the system naming, identification, enclaves, and programs are selected or applied properly.

b. Steps

i. **Expand 'Asset Findings Maint'**

ii. **Click 'Assets/Findings'**

iii. **Expand 'By Location'** and then find and expand your site/location. (Others may need to expand 'Managed By' or 'Owned By'. What is seen depends upon your permissions or role.) Within the location, assets are divided into computing, non-computing and CNDS. Proceed to step vi.
(Reviewer Only) Expand 'Visits' to display its sub-folders.

iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. **Click the 'yellow folder'** icon located at the right of 'Computing'.
You may expand 'Computing' to see assets that have already been created and that you have permissions for.

vii. **Click the 'General' tab**

- Enter the 'Host Name' following the naming convention described above.
- Enter a 'Description' of the asset. This should reflect the function and platform of the device. i.e., make and model of the device and software version etc.
- Verify/Select the location of the system in "Location"
- Verify/Select the owner of the system in "Owner": Used to register asset to parent or child location.
- Verify/Select the organization or site responsible for management of the system in "Managed By": Used for remotely managed/monitored locations.
- Verify 'Mac level', 'Confidentiality', & 'Classification', 'Status', 'Use', & 'Workstation', Change as required.
  Note: These default to MAC II, Sensitive, Unclassified, Online, Production, No. The 'Confidentiality' of a RTS system or asset should never be set to 'Public' since its configuration is considered sensitive. These settings should match those identified in the site or system SSAA.
- **Click 'Save'**.
  Note: It is recommended that you click 'Save' after filling out each tab or even more often. This practice will prevent the loss of recently entered data in the event of a timeout. You may wait to save until after filling out all tabs but you must click save at the end of data entry on all tabs or your work will be lost.

viii. **Click the 'Asset Identification' tab** to enter as much identifying information as is available:

- Enter one or all of the following: 'I.P. Address(s)', 'MAC Address(s)', 'System Unique ID'
  - **Note**: The 'System Unique ID' field may be used in addition to the IP and/or MAC addresses. The name used in the 'Host Name' field MAY be entered in the 'System Unique ID' field.
    Note: When entering IP and/or MAC addresses, complete all fields and click 'add'. The address is listed on the right. Multiple addresses can be entered one by one. Addresses can be deleted by clicking 'remove' next to the address to be deleted.
    Note: IPv6 addresses can be entered along with IPv4 addresses. Click 'IPv6' to obtain an IPv6 address box. Click 'IPv4' to revert back to an IPv4 address box. Enter as noted above.

Note: Establish your standards by using the loopback IP address of a network device. If a loopback is not used or is unavailable, use the management interface IP address or MAC address. These entries are not required if the device is not network enabled (i.e., a legacy TDM device that only has a serial management (craft) interface). In this case the device name used in the 'Host Name' field MUST be entered in the 'System Unique ID' field.

- Enter the 'Fully-Qualified Domain Name' of the device if it is a member of a network domain.
- **Click 'Save'**.

ix. **Click the 'Asset Posture' tab** to add Postures or functions to the asset:

a) **Expand 'Computing'** to view the available postures

Note: Expand each of the categories listed throughout the tree and click all applicable boxes for the specific asset being registered. Every asset has an OS. Expand 'Operating System' (and sub-branches) and select the version of OS that is used by the asset. Assets may also have applications. Expand 'Applications' (and sub-branches) and select ALL the application types and versions that are used by the asset. Follow this method for adding all applicable postures or functions to the asset being registered. The following steps will define a more detailed procedure or guide tailored to RTS systems. However, it is impossible to anticipate every possibility with these instructions due to the fact that RTS systems utilize various combinations of all technologies listed. The SA (or reviewer) is responsible for knowing what the asset being registered is, what its OS is, and what other applications or technologies it uses.

Note: Technology based rules within the VMS require the selection of additional postures and/or the input of additional information, such as instance identifiers, when selecting some items in the 'Available Postures' list. Refer to the VMS registration instructions found in the Checklist for the related technology. This is most often related to the Database and Web Server postures. A listing of these rules may be found on the VMS Help page. When this information is required, additional information or input boxes are displayed (following a 'Save) in the lower right corner of the 'Available Postures' under the 'Selected' box. Input boxes are accompanied with a 'add' link that must be clicked to enter the information.

Note: Clicking '>>' can be done after each selection or after all selections. You will need to expand the device name that appears in the 'Selected' box to see the various items selected.

Note: **Rules must be satisfied or the Asset** Posture selection(s) **will not save.** Clicking '>>' will cause any required additional input box to appear under the 'selected' box. This does NOT display alerts. Clicking 'Save' will cause an alert for any rule that is not satisfied to be displayed under the 'selected' box. Additionally, All rules and input boxes that are displayed must be satisfied before the posture will save successfully. Therefore it is recommended that '>>' and 'Save' be clicked after selecting any posture tree under the top level. The instructions will reflect this.

b) **Expand 'Voice/Video/RTS'** to view the available postures or functions.

Check all boxes that apply as follows:

Note: If registering a LAN/CAN/BAN network infrastructure device or management system, Expand 'Network' then 'Data Network' and refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.

- Check 'VoIP Switch/System/Device' if the asset provides, or is involved in providing IP based RTS communications. This includes Voice as well as VTC that is part of or associated with the Voice system. (i.e., video phones or VTC devices or applications that are controlled by or register with a RTS/VoIP LCC. This also includes IP enabled TDM switches.

AND/OR

- Check 'TDM Switch/System/Device' if the asset is a TDM based telecommunications switch. This includes IP enabled TDM that provide VoIP service. In this case 'VoIP Switch/System/Device' is also checked.

  Note: This also applies to TDM signaling a Switch/System/Device such as an SS7 STP, SSP, or SCP. (Refer to the DSN STIG for an explanation of these devices.)

OR

- Check 'Voice/Video Adjunct/Aux/Management System/Device' if the asset is involved in managing a RTS system or device or providing some adjunct or auxiliary function to the RTS system other than providing the RTS switching capability.

OR

- Check 'Video/VTC System/Device' if the asset is, or is part of, a video or VTC system that is NOT controlled by the RTS/VoIP LCC.

- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.

c) **Expand 'Role'** to view the available Roles for the asset or system being registered. Rules within the VMS require the selection of a Role.

- Check the box next to each role that the asset fulfills. RTS system devices must have one or more of the following selected:

IF the asset is part of a classified RTS system or network

- Check the box next to 'Classified RTS'. This applies to all RTS system assets including core equipment, management systems/devices and Adjunct/Auxiliary systems/devices.

OR IF the asset is used in an UN-classified RTS system

- Check the box next to 'UN-Classified RTS'. This applies to all RTS system assets including core equipment, management systems/devices and Adjunct/Auxiliary systems/devices

AND IF the asset is part of a RTS management system

- Check the box next to 'RTS Management'. This applies to assets that are part of a system that manages core equipment and/or Adjunct/Auxiliary systems/devices.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.

Note: Additional roles may need to be selected due to rules associated with other postures. One of these is the Windows OS, which requires the selection of 'Domain Controller', 'Member Server', or 'Workstation'. These may be selected now if selecting a Windows OS in the next step.

d) **Expand 'Operating System'** to view the available OSs. Drill down through the tree to locate the version of OS installed on the asset. Rules within the VMS require the selection of an OS.

- Check the box next to the OS installed on the asset. Some OSs can be found at the top level of the tree. Others and their versions require drilling deeper. The following steps provide a more in depth procedure and explanation.

IF the asset is based on a Windows OS

- Expand 'Windows' AND expand the Windows version being used.
  - Check the box next to the version of Windows installed on the asset.
    Note: For Windows registration instructions and further explanation, refer to the VMS registration instructions found in the Windows Checklist.
    Note: Rules within the VMS require the selection additional postures when selecting the Windows Operating System. This is covered in the next step.
    Note: If the version of windows being used is a vendor-customized version, check the box next to the version of Windows on which the vendor based their customization.
  - Expand 'Role' and select 'Domain Controller', 'Member Server', or 'Workstation'. RTS core equipment will typically be registered as a 'Member Server' unless it provides Active Directory Services.

Note: Rules within the VMS also add the postures of Application/Browsers/Internet Explorer/IE6 and Application/Desktop Application - General. These appear after the Role rule is satisfied and the selections/Asset is saved. The browser selection may be changed if necessary. See Browser selection below.

OR IF the asset is based on a UNIX or Linux OS

- Expand 'UNIX' AND sub-branches to locate the OS and version being used.
    - Check the box next to the version of UNIX/Linux installed on the asset.
      Note: For UNIX/Linux registration instructions refer to the VMS registration instructions found in the Unix Checklist.
      At the time of this writing, there are no rules within the VMS require the selection additional postures when selecting the UNIX or Linux Operating System.

OR IF the asset is based on a Cisco or Juniper network device OS

- Expand 'Cisco' or 'Juniper' to locate the OS and version being used.
    - Check the box next to the version of OS installed on the asset.
      Note: For Network device registration instructions refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.
      Note: Rules within the VMS MAY require the selection additional postures when selecting a Cisco or Juniper Operating System.

OR IF the asset is based on a embedded network device OS and/or has not been located anywhere else in the OS tree:

- Expand 'Network Device Embedded OS' to locate the OS and version being used.
    - Check the box next to the version of OS installed on the asset.
      Note: For Network device registration instructions refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.
      Note: Rules within the VMS MAY require the selection additional postures when selecting a Network Device Embedded OS. **IF** the appropriate OS has not been located anywhere else in the OS tree, Check the box next to 'Other Network OS'
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
    - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
    - Satisfy any Rule alert that appears under the 'Selected' box.
    - Click **'>>'** and **Save'** again.

e) **IF** the asset is a server or a piece of RTS system core equipment, proceed to f) and select all the applications used by the devise as follows;
ELSE skip to "g)" below

f) **Expand '<u>Application</u>'** to view the available applications. Drill down through the tree to locate all applications and versions being used by the asset. This is a required step to define what applications are installed on the asset for which there is configuration guidance or for which IAVM notices exist. This requirement is typically applicable to RTS core equipment and servers. The SA (or reviewer) is responsible for knowing what general-purpose applications the asset being registered uses or is based upon. The SA (or reviewer) is further responsible for selection all general-purpose applications that the asset being registered uses. The following steps will detail applications that are typically found as the basis of or used by RTS assets.

- **Expand '<u>Database</u>'** and drill down to find the version of database being used on the asset. If not used or not found; skip this selection.
    - Check the box next to the version of Database being used on the asset. **<u>Note</u>**: For Database registration instructions refer to the VMS registration instructions found in the Database Checklist. **<u>Note</u>**: Rules within the VMS require the selection additional postures when selecting a Database.
- **Click '<u>>></u>'** to move the posture to the 'Selected' window (Optional/Recommended)
    - Enter any additional information requested by the appearance of an input box under the '<u>Selected</u>' box. Click '<u>Add</u>'.
- **Click '<u>Save</u>'**. (Optional/Recommended)
    - Satisfy any Rule alert that appears under the '<u>Selected</u>' box.
    - Click **'<u>>></u>'** and **<u>Save</u>'** again.
- **Expand '<u>Web Server</u>'** and drill down to find the version of Web Server being used on the asset. If not used or not found; skip this selection.
    - Check the box next to the version of Web Server being used on the asset. **<u>Note</u>**: For Web Server registration instructions refer to the VMS registration instructions found in the Web Server Checklist. **<u>Note</u>**: Rules within the VMS require the selection additional postures when selecting a Web Server.
- **Click '<u>>></u>'** to move the posture to the 'Selected' window (Optional/Recommended)
    - Enter any additional information requested by the appearance of an input box under the '<u>Selected</u>' box. Click '<u>Add</u>'.
- **Click '<u>Save</u>'**. (Optional/Recommended)
    - Satisfy any Rule alert that appears under the '<u>Selected</u>' box.
    - Click **'<u>>></u>'** and **<u>Save</u>'** again.
- **Expand '<u>Application Servers</u>'** and drill down to find the version of Application Server being used on the asset. This will typically be a version of Tomcat. If not used or not found; skip this selection.
    - Check the box next to the version of Application Server being used on the asset. **<u>Note</u>**: For Application Server registration instructions refer to the VMS registration instructions found in the Web Server and Application Checklists.

Note: Rules within the VMS require the selection additional postures when selecting an Application Server.

- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'Browsers'** and drill down to find the version(s) of Browser(s) being used on the asset. If not used or not found; skip this selection.
  Note: If a browser was automatically added to the asset's posture when selecting a Windows OS and it is the correct browser, skip this selection. If not, select the proper browser, add it, and select the incorrect browser version and click '<<' to remove it.
  - Check the box next to the version of Browser being used on the asset.
    Note: For Browser registration instructions refer to the VMS registration instructions found in the Web Checklist and/or Desktop Application Checklist.
    Note: Rules within the VMS require the selection additional postures when selecting a Browser.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'Antivirus'** and drill down to find the version of Antivirus being used on the asset. If not used or not found, skip this selection. The use of Antivirus software is a requirement for all Windows based systems.
  - Check the box next to the version of Antivirus being used on the asset.
    Note: For Antivirus software registration instructions refer to the VMS registration instructions found in the Desktop Application Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting Antivirus Software.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
- **Expand 'JVM'** and drill down to find the version of Java Virtual Machine Manager being used on the asset. If not used or not found; skip this selection. This is required, however, when registering certain other web server postures.

  - Check the box next to the version of ESM software being used on the asset.
    Note: For JVM registration instructions refer to the VMS registration instructions found in the Web Server Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting a Java Virtual Machine.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'MSdotNETFramework'** and drill down to find the version of Framework being used on the asset. If not used or not found; skip this selection.
  - Check the box next to the version of Framework being used on the asset.
    Note: For dotNET Framework registration instructions refer to the VMS registration instructions found in the Web Server Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting a dotNET Framework.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'ESM'** and drill down to find the version of Enterprise System Manager being used on the asset. If not used (not typically used) or not found; skip this selection.
  - Check the box next to the version of ESM software being used on the asset.
    Note: For ESM registration instructions refer to the VMS registration instructions found in the ESM Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting ESM software.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.

- **Expand '<u>Office Automation</u>'** and drill down to find the version of Office Automation software being used on the asset. If not used (not typically used) or not found; skip this selection.
  - o Check the box next to the version of Office Automation software being used on the asset.

    <u>Note</u>: For Office Automation registration instructions refer to the VMS registration instructions found in the Desktop Application Checklist.

    <u>Note</u>: Rules within the VMS MAY require the selection additional postures when selecting an Office Automation.
- **Click '<u>>></u>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - o Enter any additional information requested by the appearance of an input box under the '<u>Selected</u>' box. Click '<u>Add</u>'.
- **Click '<u>Save</u>'**. (Optional/Recommended)
  - o Satisfy any Rule alert that appears under the '<u>Selected</u>' box.
  - o Click **'<u>>></u>'** and **<u>Save</u>'** again.

g) **IF** registering a network switch, router, or other network transmission element, that is part of a LAN supporting an Adjunct or Auxiliary system or the management of the RTS system or an Adjunct or Auxiliary system, AND it is NOT part of the BCPS LAN/CAN/BAN/WAN network infrastructure or management system, proceed to h) below:
ELSE skip to i) below:

h) Expand '<u>Network</u>' then '<u>Data Network</u>' and refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.

- Check the boxes next to the appropriate postures for the asset.
- **Click '<u>>></u>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - o Enter any additional information requested by the appearance of an input box under the '<u>Selected</u>' box. Click '<u>Add</u>'.
- **Click '<u>Save</u>'**. (Optional/Recommended)
  - o Satisfy any Rule alert that appears under the '<u>Selected</u>' box.
  - o Click **'<u>>></u>'** and **<u>Save</u>'** again.

i) **Click '<u>Save</u>'** one last time Proceed to x.

x. **Click the '<u>Functions</u>' tab** to select the function of the asset being registered.
- o Select all functions that the asset performs. If an appropriate function is not found; skip this selection.
- o Click '<u>>></u>' to move it to the '<u>Selected</u>' window.
- o Click '<u>Save</u>'

xi. **Click the '<u>Systems / Enclaves</u>' tab** to associate this asset with the appropriate or all applicable program(s), enclave(s), and site(s).
- o In the '<u>Available Systems</u>' box:
  - Find and select '<u>DISN-DSN</u>' if the system can place or receive DSN calls.

  OR
  - Find and select '<u>DISN-DRSN</u>' if the system can place or receive DRSN calls.

- Click '>>' to move it to the 'Selected Systems' window
- IF the RTS System is managed or monitored by the ADIMSS (DSN), Find and select 'ADIMSS'

OR

- IF the RTS System is managed or monitored by the ARDIMSS or ESRS (DRSN), Find and select 'ARDIMSS' and/or 'ESRS'
- Click '>>' to move it to the 'Selected Systems' window

o In the 'Available Enclaves' box:

- Find and select the local enclave that the RTS system is part of. (i.e., your site/location) (These selections may not in the list as yet)
  Note: For registered enclaves, choose the enclave. If the enclave is not present, your IAM to determine if the enclave has been requested to be added. [*(Reviewer Only)* contact your team lead.] If the team lead or IAM has requested an enclave be added; 'Select Has Been Requested'. If the enclave has not been requested; 'Select Not Available'. There should not be any assets registered/updated that are not part of an enclave.

o Click '>>' to move it to the 'Selected Systems' window

o Click 'Save'

xii. **Click the 'Additional Details' tab** and provide all of the requested information for the RTS asset; Building and room number should reflect the actual location of the RTS of the asset. Other information requested is Serial Number and Barcode, Make, Model and Manufacturer.

xiii. **Click 'Save'**.

xiv. Return to step vi to create another Computing asset or proceed to Reviewing Assets in the next section.

Note: (Reviewer) New assets created by a reviewer will be found under the 'Not Selected for Review" area of the visit tree for the site that the asset is registered to.

Note: (Reviewer) Changing the status of one vulnerability will move the asset from the 'Not Selected for Review" area or the 'Must Review' area to the 'Reviewed" area of the visit tree for the site that the asset is registered to.

Note: When creating a NEW asset it is recommended to run a VL03 report to identify the IAVMs that will be assigned to the new asset being created. (See instructions below). IAVMS that are assigned to an asset will default to an open status and must be acknowledged and fixed immediately. All other vulnerabilities will default to 'Not Reviewed'

Note: The following process may be used in the event that there is a need to create multiple assets having the **same** configuration or postures.
CAUTION: Extreme care must be exercised when performing this procedure. The identifying information MUST be changed (as listed under "minimum edit" below). If this information is not changed, the exported asset will be updated only.

- Create the first asset and save it.

- While displaying the first asset's registration information, export the asset. This will create a .xml file on your computer that contains the registration information.
- Open the .xml file in a text editor.
- Edit the identifying information for the asset.
  - At a minimum edit the following:
    - Asset name
    - Host name
    - Unique ID
    - MAC Address
    - IP address
  - Optionally edit the following:
    - Building
    - Room
    - Serial number
    - Barcode
- Save the edited information insuring that the file name is changed appropriately and the .xml extension is maintained.
- Return to VMS and click the XML icon to the right of the file folder icon nest to computing. Browse for the file and click submit.
- Open the newly created asset and update/validate all identification and posture information. Update as needed.

1.7 Reviewing Assets – Step-by-Step

Note: The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. This will also identify the assets that have been created and can help to eliminate the creation of duplicate assets (i.e., the same asset under different names) Instructions for generating this report are provided under "Additional Reports" below.

1.7.1 First Review of the Asset under VMSv6

When reviewing an asset for the first time under VMSv6 or after initial registration in VMSv6, all asset registration and posture information must be validated. This occurs under the following conditions.

- The asset had been registered in VMSv5.4 and has been brought forward into VMSv6.
  - o Additional information as well as the asset postures must be added.
- An SA has initially registered the asset under VMSv6 and a Reviewer will be performing a review on the asset.
  - o The reviewer must validate that all information and applicable postures have been properly assigned to the asset. The reviewer must work with the SA to insure proper and complete registration occurs.

c. *Steps*

i. **Expand '<u>Asset Findings Maint</u>'**

ii. **Click '<u>Assets/Findings</u>'**

iii. ***<u>(SA)</u>*** **Expand <u>'By Location'</u>** and proceed to step vi.
(Reviewer Only) Expand '<u>Visits</u>' to display its sub-folders

iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. **Expand '<u>Computing</u>'**.

vii. *(Reviewer Only)* **Expand '<u>Must Review</u>'**
SA will not see '<u>Must Review</u>', but will proceed to step viii.

viii. **Click the '<u>Asset Name</u>'**.
- o Verify data in '<u>General</u>' tab and '<u>Asset Identification</u>'.
For details see Section 1 "Creating the Asset", steps vii and vii.

ix. **Click the '<u>Asset Posture</u>' tab** verify the postures/functions assigned to the asset:
- o Expand 'The <u>Asset Name</u>' in the 'Selected ' window (if it's there.)
- o Verify that all postures for the asset has been selected and are accurate.
- o IF the asset is not shown in 'Selected' box, or the postures are not accurate, see Section 1 "Creating the Asset", step ix.
<u>Note</u>: Assets registered under VMSv5.4 may have an OS assigned, but the additional postures/functions will have to be assigned.

x. **Click the '<u>Functions</u>' tab**

  - o Verify that all Functions for the asset has been selected and are accurate. See Section 1 “Creating the Asset”, step x. (As of 4/7/06 there are no RTS specific functions. This step may be skipped at this time.)

xi. **Click the ‘<u>Systems / Enclaves</u>’ tab**.

  - o Verify that the asset has been associated with the appropriate or all applicable program(s), enclave(s), and site(s). See Section 1 “Creating the Asset”, step xi.

xii. **Click the ‘<u>Additional Details</u>’ tab**

  - o Verify that the information on this tab is accurate. See Section 1 “Creating the Asset”, step xii.

xiii. If any of the information found is inaccurate, See Section 1 “Creating the Asset” for instructions on making additions or changes.

xiv. <u>Continue with the following section</u> ‘Procedures for Review of the Asset’ step vii ‘Must Review’

1.7.2 Procedures for Updating the Vulnerability Status of the Asset

If all registration tasks have been accomplished and/or verified, use the following procedures for updating the status of all assets, both computing and non-computing:
Note: (*Reviewer Only*) In the event that the Voice/Video/RTS asset just reviewed does not exist in VMS, the reviewer may create it. It is highly recommended that the reviewer have the Voice/Video/RTS SA create the asset and then work with him/her to assure that the asset is fully and properly registered and named or identified in accordance with the Voice/Video/RTS asset registration instructions described above. If a reviewer must create an arbitrary asset to enter his/her vulnerability statuses, he/she must notify the team lead, others on the team that may also have to update their statuses on the same asset, and the Voice/Video/RTS asset SA. The Voice/Video/RTS asset SA may then update the registration information as needed. Additionally, the reviewer should check with the Voice/Video/RTS asset SA before creating a new asset in the event that the asset does exist in VMS but shows up in a different part of VMS. (i.e., identified differently or registered to a different organization). If a reviewer creates an asset, he/she becomes the SA or "owner" for the asset. "Ownership" of assets created by a reviewer must be transferred to the actual SA for the asset.

d. *Steps*

i. **Expand 'Asset Findings Maint'**

ii. **Click 'Assets/Findings'**

iii. ***(SA)*** **Expand 'By Location'** and proceed to step vi.
(Reviewer Only) Expand 'Visits' to display it's sub-folders

iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. **Expand 'Computing'** and/or **'Non-Computing' and/or 'CNDS'** as applicable

vii. *(Reviewer Only)* **Expand 'Must Review'**
SA will not see 'Must Review', but will proceed to step viii.
Note: (*Reviewer Only*) Newly created assets will appear under "Not Selected for Review".

viii. **Expand the ' Asset Name'** for the asset to be reviewed. The icon in front of "Ready to review" assets is colored in RED. Drill down until the list of vulnerabilities displays under the asset. If multiple postures were selected for the asset during registration, a list of the postures is displayed. Expand each posture to see the list of vulnerabilities under each.
Note: Determine what postures, if any, can be reviewed and updated using automation. This would apply to any posture / technology for which a Gold Disk or a set of review scripts exist. (i.e., Windows Gold disk(s), and scripts for Unix, Database, and Web Servers). It is highly recommended that this automation be used to review as many findings as possible before beginning a manual review or update of the remaining vulnerabilities. Once reviewed in this manner, the results are imported into VMS to update the status of the vulnerabilities for each set of automation or technology. All vulnerabilities may be updated manually.

Note: To review / update all vulnerabilities under all major postures or technologies other than Voice/Video/RTS, Refer to the Asset Review instructions found in the appropriate checklist for that technology.
Note: When you drill down into the lowest level of the asset tree, you will find the Vulnerabilities and IAVMs assigned to the asset.

ix. **Click on a '<u>Vulnerability Key</u>'** in the tree that needs to be updated to open its status update area and tabs (scroll down to see if necessary).

x. **On the '<u>Status</u>' Tab**, Update the 'Status' of the vulnerability.
Note: If selecting a status of '<u>O-Open</u>', a '<u>Details'</u> and '<u>Milestone</u>' must also be entered.

xi. **Click the '<u>Details</u>' Tab**, (Conditional) identify details on all open vulnerabilities/findings by adding to or modifying the default details displayed in the box.

xii. **Click the '<u>Comments</u>' Tab**, (Optional) Add ,any pertinent comments

xiii. **Click the '<u>Programs</u>' Tab**, (Conditional)
Note: This is a place holder for future instructions relating to Program Baselines

xiv. **Click the '<u>POA&M</u>' Tab**, (*SA, not Reviewer*) (Conditional)
Note: SAs performing self-assessments are required to enter a POA&M for all open vulnerabilities/findings before the status will save. This does not apply to a reviewer.
- o Click the '<u>New Milestone</u>' Button, Enter a '<u>Milestone</u>' (description of a step in mitigating/fixing the finding) and a '<u>Completion Date</u>'.
- o Click the '<u>Disk/Save</u>' icon on the left to save the milestone
- o Enter additional milestones as necessary.

xv. **Click the '<u>Apply to Other Findings</u>' Tab**, (Conditional) If applicable: Check '<u>Choose Other Assets with the Same Finding in the Same Status</u>'. Select the appropriate assets.
Note: If this feature of VMS is to be used, it must be used before clicking '<u>Save</u>' or else no assets with similar postures / statuses will be found.

xvi. **Click the '<u>Save</u>'** button at the bottom of the form area
Note: Alert messages will be shown below the '<u>Save'</u> Button. If alert messages display, the status update information will not save until the alert message(s) is satisfied.

xvii. Return to step ix above and select another '<u>Vulnerability Key</u>'. Repeat this until all '<u>Computing</u>' and '<u>Non-Computing</u>' asset vulnerability statuses are updated.
Note: System Administrators should expand the OS assigned to the asset and each IAVM. Verify the OS level meets the required release or patch level.

1.7.3 Verify that all necessary assets were reviewed

e. Steps

i. **Expand '<u>Asset Findings Maint</u>'**

ii. **Click '<u>Assets/Findings</u>'**

iii. ***<u>(SA)</u>*** **Expand <u>'By Location'</u>** and proceed to step vi.
(Reviewer Only) Expand '<u>Visits</u>' to display it's sub-folders

iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. **Expand '<u>Computing</u>'** and/or **'Non-<u>Computing</u>' and/or '<u>CNDS</u>'** as applicable

vii. *(Reviewer Only)* **Expand '<u>Must Review</u>'**
SA will not see '<u>Must Review</u>', but will proceed to step viii.

viii. **Expand Each 'Asset Name'** to view the list of asset postures.
- If checkmarks are gone, the asset has been fully reviewed.

ix. **Done**

The following reports can be used to verify the status of the site and its assets.

1. VC06 Asset Compliance Report
   a. A Full report may be obtained
2. VC03 Severity Summary Report
   a. Table of numbers only
3. VC01
   a. Used for IAVM Compliance

See **Compliance monitoring** below for a quick set of instructions on generating these reports.

1.7.4 Add Comments to a Visit (Reviewer only)

f. *Steps– Click the following:*

i. '<u>Visit Maint</u>.'
ii. Expand the Organization the visit is set up for.
iii. Expand the Visit
iv. Locate the visit you are working on. (Drill down till you find it)
v. Click on CCSD or enclave name. (Drill down till you find it)
vi. '<u>Comments Tab</u>'
   a) Type your comments
vii. '<u>Save Changes</u>'

1.8 Reports – Step-by-Step

1.8.1 Compliance Monitoring

- **VC06 –** provides a detailed report of all vulnerabilities that are assigned to an asset and its postures. There are many items that can be selected for display and the report can be filtered and sorted in multiple ways.

  g. *Steps– Click the following:*

  i. ‘Reports’
  ii. ‘VC06’
  iii. Select an ‘Asset(s)’ or an ‘Organization(s)’.
  iv. Select “open” status to see only “Open” findings (Select others as desired. Hold the Ctrl or Shift key to make multiple selections)
  v. Select the sort order under ‘Sort By’
  vi. Select the information to be displayed: Check the following boxes:
     4. ‘Finding Comments’
     5. ‘Finding Long Name’ (Because it’s truncated otherwise)
     6. ‘Finding Details’
     7. ‘Vulnerability Discussion’
     8. Others as desired
  vii. ‘Generate Report’

- **VC03 –** Provides a table of assets and technologies with the number and percentage of findings against each listed by severity category. Has numbers only.

  a. *Steps– Click the following:*

  i. ‘Reports’
  ii. ‘VC03’
  iii. Select an ‘Organization(s)’
  iv. Review other options and select as desired
  v. ‘Generate Report’

- **VC01 -** Used for IAVM Compliance (An SA may not see this option)

  a. *Steps– Click the following:*

  i. ‘Reports’
  ii. ‘VC01’
  iii. On the ‘Organizations’ Tab, Select an organization
  iv. On the ‘Vulnerabilities’ Tab, Select IAVM(s) or year(s)
  v. Review other options and select as desired
  vi. ‘Generate’

1.8.2 Additional Reports

The following reports can be used for identifying assets at a site or location and determine what IVAMs are related to specific assets. Quick step by step instructions for creating the reports follows.

- **AS01 - Identifying Assets**
  Note: The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. These instructions are applicable to locating all assets but are geared toward Telecom/RTS assets.
  a. Steps – Click the following:
    i. ‘Reports’
    ii. ‘AS01’
    i. Select ‘Computing’, hold Ctrl key, and select ‘Non-Computing’ (SUBMIT)
    ii. Select ‘By Location’ (SUBMIT)
    iii. Select the location
      1. May want to do other reports if your site manages or owns assets that are not located at their site. Check the box for Child Locations if applicable. (SUBMIT)
    iv. Expand ‘Non-Computing’
      1. Check the box for ‘Telecom Policy’
    v. Expand ‘Computing’.
      1. Check the box for ‘Telecom’
    vi. Select ‘Online’, ‘Offline’, or ‘Both’. Located under the right calendar (‘Both’ is recommended but ‘Online’ is the default)
    vii. Check the box for ‘Show Detailed Asset Information’ (Recommended - This will show a tree display of all postures that have been assigned to the asset during registration)
    viii. Check the box for ‘Show System Administrator Information’ (Recommended)
    ix. Submit to receive the Telecom/RTS Asset Report
    Note: Reports are best displayed using the ‘Output / Screen’ option. The display may then be printed. Clicking the IE6 print function prints the report only without the surrounding frames. Using the ‘Output / Export file’ option produces a tab delimited text file. This file can be opened with excel to receive a database like table of the information. Use Right Click/Open With in Windows to open the file.

- **VL03 - Look at IAVMs assigned to an Operating System or Application**
  Note: The VL03 report can assist the review by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. This can be accomplished by performing the following steps.
  a. Steps– Click the following:
    i. ‘Reports’
    ii. ‘VL03’
    x. Select ‘Select by Operating System/Application(s)’
    xi. Select the OS(s) and Applications(s) to report on

xii. Select the environment (SUBMIT)
xiii. Select any additional display options or deselect the default selections
iii. <u>‘Generate Report’</u>

VoIP 0020 V0008222 CAT II LAN Not Enclave and Network STIG compliant

8500.2 IA Control:	ECSC-1
Vulnerability	The VoIP system is not compliant with overall network security architecture and appropriate enclave security requirements.
Vulnerability Discussion:	Requirement: The IAO will ensure that the network supporting IPT implementations (i.e., the underlying data network) is configured to comply with the Network Infrastructure and Enclave STIGs. Network security to include filtering and monitoring are essential elements of a modern VoIP network architecture. This is especially important for voice with the transition from the data network to the VoIP network environment. The two most important forms of protection against unauthorized use of common user communications networks are packet filtering and monitoring. If these do not exist, this would present exposure to new threats, such as communications traffic interception, modification, insertion and denial of service. It is imperative that all measures be taken at the network architectural level to ensure the security of telephony traffic in the IP environment. Guidance for this should be obtained from the Network Infrastructure and Enclave Security STIGs in addition to this STIG.
References:	Voice Over Internet Protocol (Voip) STIG V1R1 Para 1.0
Checks:	> Review Network & Enclave SRR results (Manual) - Review the results of the most recent Enclave and Network Reviews. If there are a significant number of findings reported or if these STIGs were not applied, this is a finding.
Fix(es):	> Perform Enclave and Network Reviews (Manual) > Review the VoIP environment using the Network Infrastructure and Enclave STIGs / Checklists. Ensure firewall filtering and intrusion detection monitoring are in place according to guidance. > Upgrade/configure the LAN (Manual) > Upgrade the LAN infrastructure as necessary to meet Network Infrastructure and Enclave STIG requirements.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0025 V0008302 CAT III IPT / VoIP LAN cannot support C2 assured service

8500.2 IA Control: ECSC-1

Vulnerability The LAN supporting IPT / VoIP is not designed or implemented as a DOD C2VG LAN in accordance with the DOD GSCR, Appendix 3 and therefore cannot support assured service in support of C2 reliability requirements.

Vulnerability Discussion: equirement: The IAO will ensure that the network supporting IPT implementations (i.e., the underlying data network) is designed and implemented as a DOD C2VG LAN or ASCLAN and will possess bandwidth, reliability, survivability, and prioritization capabilities in accordance with the DOD GSCR, Appendix 3 and/or ASCLAN GSR.

Voice services in support of C2 and Special C2 users are required to meet certain minimum requirements relating to reliability and survivability of the supporting infrastructure. Design requirements for networks supporting DOD IPT/VoIP implementations can be found in the DOD Generic Switching Center Requirements (GSCR) document in Appendix 3. This Appendix contains the specifications for a Command and Control Voice Grade LAN (C2VG LAN) required to support DOD IPT. These specifications define LAN design requirements for redundancy of equipment and their interconnections as well as minimum requirements for bandwidth and backup power.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3
DOD Generic Switching Center Requirements (GSCR), 8 September 2003

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review Network Diagrams - C2 LAN (Manual)> Interview the IAO and review site network/facilities diagrams and documentation to confirm compliance.

Specific attention should be given in the areas of:

- Equipment redundancy above the access layer
- Connection redundancy above the access layer
- Equipment robustness and bandwidth capability
- Connection bandwidth capability
- Access layer switch size / number of phones served is below maximum
- Backup power for all equipment.

o Support for C2 users requires 2 hours minimum for all supporting equipment.
o Support for Special C2 users requires 8 hours minimum for all supporting equipment.

Fix(es): > Comply with Policy - C2 LAN (Manual) (Manual)>- Upgrade the LAN infrastructure as necessary to meet requirements.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0030 V0008223 CAT II The IPT/ VoIP system not in the site's SSAA

8500.2 IA Control: DCHW-1

Vulnerability VoIP devices exist that have not been added to site System Security Authorization Agreements (SSAAs).

Vulnerability Discussion: Requirement: The IAO will ensure that VoIP devices are added to site System Security Authorization Agreements (SSAAs).

Documentation of the enclave configuration must include all VoIP systems. If the current configuration cannot be determined then it is difficult to apply security policies effectively. Security is particularly important for VoIP technologies attached to the enclave network because these systems increase the potential for eavesdropping and other unauthorized access to network resources. Accurate network documentation is critical to maintaining the network and understanding its security posture, threats, and vulnerabilities. An SSAA is the vehicle by which the DAA receives security related information on the network for which he/she is personally responsible and accepts the security risk of operating the system.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3
DOD 8510.1-M; DITSCAP Application Manual

Checks: > Review the SSAA (Manual)> Review the SSAA and verify that all VoIP installations or modifications are included. Verify there is a procedure for approving changes to configuration.

Fix(es): > Add all VoIP installations to the SSAA (Manual) > Add all VoIP installations and/or modifications to the SSAA. Obtain DAA approval for the updated SSAA. Submit to the SRR team lead for validation and finding closure.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0035 V0008285 CAT II IPT / VoIP LAN NOT DSN STIG compliant

8500.2 IA Control: ECSC-1

Vulnerability The IPT / VoIP system is not compliant with the overall DOD voice system requirements contained in the DSN STIG.

Vulnerability Discussion: Requirement: The IAO will ensure that VoIP systems are compliant with the DSN STIG.
Specific emphasis to be given in the following areas:
- System certification, accreditation, and listing on the DSN APL in accordance with the DODI 8100.3
- Site administrative requirements
- Requirements for management of voice systems and management interfaces.
- This list is not all-inclusive.

Many of the requirements that apply to all voice systems are contained in the DSN STIG. AS such any IPT/ VoIP system must be in compliance with the overall DSN / DOD Voice system requirements.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3
Defense Switched Network STIG V2R1

Checks: > Review DSN SRR results (Manual) - Review the results of the most recent DSN SRR or Self Assessment. If there are a significant number of findings reported or if the DSN STIG was not applied, this is a finding.

Fix(es): > Perform a DSN review (Manual) - Review the VoIP environment using the DSN STIG / Checklist for compliance. Ensure firewall filtering and intrusion detection monitoring are in place according to guidance. Upgrade the LAN as necessary to meet requirements.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0040 V0008224 CAT II MGCP is being used without IPSEC

8500.2 IA Control: ECCT-1: ECNK-1: ECSC-1

Vulnerability MGCP is being used without IPSEC enabled on each the MGCs to provide authentication and encryption.

Vulnerability Discussion: Requirement: If MGCP is used, the IAO will ensure that IPSEC is enabled on each of the MGCs to provide authentication and encryption. Media Gateway Control Protocol (MGCP) is a protocol that is used between Media Gateways to exchange sensitive gateway status and zone information. MGCP is a clear text protocol. This information is critical in the setup and completion of voice calls from VoIP zone to VoIP zone. If this information is poisoned or if collected and used by an unauthorized unscrupulous individual, the effects to the VoIP environment could be detrimental. In addition, (RFC) 2705 (MGCP) outlines and recommends the use of IPSEC for encryption and authentication between gateways. Since this feature is inherent to the protocol, good security practice dictates its use.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.12

Checks: > IAO/SA demonstrate IPSEC on MGCP (Manual) > Inspect, or have site personnel demonstrate compliance on, a sampling of effected devices to confirm compliance. Request the SA demonstrate that IPSEC is enabled for MGCP signaling on Media Gateways, Media Gateway Controllers, and other devices such as end instruments if they use MGCP, by providing configuration details.

Fix(es): > Enable IPSEC for MGCP (Manual) > Enable IPSEC for MGCP signaling on Media Gateways, Media Gateway Controllers, and other devices such as end instruments that use the Media Gateway Control Protocol.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0050 V0008225 CAT II Improper Physical security - System access

8500.2 IA Control: ECSC-1

Vulnerability Critical VoIP network and server components are NOT located in secured areas.

Vulnerability Discussion: Requirement: The IAO will ensure all critical VoIP network and server components are located in a secured area. This does not apply to end instruments.

Controlling physical access to the VoIP network and server components is critical to assuring the reliability of the voice network and service delivery.

Documenting or logging physical access to the VoIP network and server components is critical to determine accountability for auditing purposes.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.2

Checks: > Confirm physical security (Manual) > During a walk through inspection, visually confirm that VoIP network and server components are installed in secured areas to include locked rooms, closets, and/or cabinets. Interview the IAO to determine how the distribution of keys to access the equipment is limited, controlled, and documented. Additionally determine if access control procedures/documentation are/is being used and review the access logs for compliance.

Fix(es): > Establish Physical Security (Manual) > The IAO must ensure that all equipment is installed in a locked room, closet, or cabinet. Additionally the IAO must insure that the distribution of keys to access the equipment is limited, controlled, and documented. Additionally, access control procedures should be implemented to insure that physical access is documented so that an audit trail can be established if necessary.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0060 V0008226 CAT III Network configuration is displayed on IP phones

8500.2 IA Control: ECSC-1

Vulnerability IP phones are configured to display network IP configuration information without the use of a password.

Vulnerability Discussion: Requirement:
The IAO will ensure that IPT terminals (VoIP phones or instruments) cannot be configured at the terminal and do not display network/terminal configuration information on their display without the use of a password.

Some IP phones display VoIP network information making it easy to collect VoIP network information that could be used by would be hackers / attackers. Therefore these devices should be considered a target to be defended against such individuals that would collect voice network information for illicit purposes. To help prevent against information gathering by the unscrupulous, measures must be taken to protect this information. Programming IP Phones not to display Network information (i.e. IP address, subnet mask, gateway, LCC addresses or URLs, etc.), without entering a password or PIN code, should be considered another layer of security in protecting the VoIP environment.

Potential Impacts: Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. System or server attack based on information gathered from end instruments.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.3

Checks: > Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fix(es): > Properly configure IP Phones (Manual) > Configure IP Phones to NOT display voice network information without the entry of a password or a PIN code.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0061 V0008287 CAT III Phone passwords/PINs do not remote authenticate

8500.2 IA Control: ECSC-1

Vulnerability The IPT terminal’s configuration/configuration-display passwords/PINs DO NOT authenticate remotely to the IPT system controller (Local Call Controller (LCC)).

Vulnerability Discussion: Requirement: The IAO will ensure that the IPT terminal’s configuration/configuration-display passwords authenticate remotely to the IPT system controller (Local Call Controller (LCC)).

Passwords or PIN codes used to access an IPT / VoIP terminals or end instruments configuration menu or display should not be stored on the terminal or end instrument. They should be stored on the system controller. The terminal or end instrument should query the system controller for password or PIN code authentication. In this way, passwords and PIN codes can be managed and changed as necessary to comply with password management policy.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.3

Checks: > Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Configure the system for compliance (Manual) – Configure the system for compliance if the feature is available. Vendors should provide this capability in their systems

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0062 V0008288 CAT II There is NO IPT / VoIP terminal PIN policy

8500.2 IA Control: ECSC-1, IAIA-1, IAIA- 2

Vulnerability There is NO IPT / VoIP terminal password/PIN management policy.

Vulnerability Discussion: Requirement: The IAO will ensure that a policy is in place to ensure that the IPT terminal (VoIP phone or instrument) configuration and display password is managed IAW DOD password policies (e.g., password complexity, expiration, reuse, protection and storage).

PINs that are not managed or reqired to be changed are most likely never chaned, therefore they are easily compromised or guessed.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.3

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation,Configuration files, DAA approvals, etc as applicable.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0065 V0008289 CAT II Auto-reg. of VoIP terminals NOT disbled

8500.2 IA Control: ECSC-1

Vulnerability Auto-registration of VoIP terminals is NOT disabled.

Vulnerability Discussion: Requirement: The IAO will ensure that auto-registration of VoIP terminals is disabled within 5 days following initial system setup and/or following any subsequent large redeployments or additions.

The Auto-registration feature provided in some IPT / VoIP systems presents various issues. In general this feature allows any end instrument to function using a default configuration as soon as it is plugged into the network without prior authorization and configuration by an SA. In general this feature should never be used even in the limited situations mentioned in the requirement since the SA loses control of the system. In this situation the SA may not know what phones are on the system or where they are and since phone numbers are usually assigned out of a pool, there is no SA control over number assignments. Additionally since end instruments can work as soon as plugged in, they could be used to abuse the phone system.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.4

Checks: > Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0066 V0008290 CAT II NO Inventory of authorized instruments

8500.2 IA Control: ECSC-1

Vulnerability An inventory of authorized instruments is NOT documented or maintained.

Vulnerability Discussion: Requirement: The IAO will ensure that an inventory of authorized instruments is documented and maintained.

It is critical to the security of the system that all IPT /VoIP end instruments be authorized to connect to and use the system. Only authorized instruments should be configured in the system controller and therefore allowed to operate. Unauthorized instruments could lead to system abuse.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.4

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.
> Inspect/Review Documents (Interview) > Inspect or review the required “documents on file” that are necessary for compliance with the requirement.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0067 V0008291 CAT II UN-authorized terminals are registered

8500.2 IA Control: ECSC-1

Vulnerability UN-authorized VoIP terminals are registered With the LCC and are operational

Vulnerability Discussion: Requirement: The IAO will ensure that the VoIP system only registers authorized terminals. This can be through an automated authorization process during auto-registration or by comparing the registration logs to the documented authorized inventory following any usage of auto-registration.

It is critical to the security of the system that all IPT /VoIP end instruments be authorized to connect to and use the system. Only authorized instruments should be configured in the system controller and therefore allowed to operate. Unauthorized instruments could lead to system abuse.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.4

Checks: > Perform a walk-through (Manual) > Perform a walk through of the facility to confirm compliance via inspection of the effected devices or items
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Remove unauthorized phones (Manual) > Remove unauthorized terminals, phones, endpoints etc from the VoIP network.
> Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0068 V0008293 CAT II Manual registration of VoIP terminals NOT used

8500.2 IA Control: ECSC-1

Vulnerability Manual registration of VoIP terminals is not being used for normal operations

Vulnerability Discussion: Requirement: The IAO will ensure that manual registration of VoIP terminals is used for normal, day-to-day, troubleshooting and repairs, or moves, adds, and changes.

It is critical to the security of the system that all IPT /VoIP end instruments be authorized to connect to and use the system. Only authorized instruments should be configured in the system controller and therefore allowed to operate. Unauthorized instruments could lead to system abuse.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.4

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Configure for manual registration (Manual) - Configure the LCC for manual registration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0070 V0008227 CAT II VoIP system is not addressed differently than data

8500.2 IA Control: DCPA-1: ECSC-1

Vulnerability VoIP systems and components are not deployed on a logically segregated Subnet with different IP addressing from the data network.

Vulnerability Discussion: Requirement: The IAO will ensure that all VoIP systems and components are deployed on their own dedicated IP network(s) or sub-network(s) that utilize separate address blocks from the normal data address blocks thus allowing traffic and access control via firewalls and router ACLs.

The combination of logical data and voice segmentation via addressing and VLANs coupled with a switched and routed infrastructure strongly mitigates call eavesdropping and other attacks. In addition, limiting logical access to VoIP components is necessary for protecting telephony applications running across the infrastructure. Segregating data from telephony by placing VoIP servers and subscriber terminals on logically separate IP networks while controlling access to these VoIP components through IP filters will help to ensure security and aid in protecting the VoIP environment.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fix(es): > Segregate VoIP systems - IP Addressing (Manual) > Implement VoIP systems and components on a logically segregated and dedicated telephony (VoIP) network using IP address space that is different than the general data network.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0080 V0008228 CAT III VoIP system does not use RFC 1918 addressing

8500.2 IA Control: DCPA-1: ECSC-1

Vulnerability VoIP systems are not deployed on a "private" (non WAN routed) network in accordance with Request for Comments (RFC) 1918.

Vulnerability Discussion: Requirement: The IAO will ensure that all local VoIP systems and components are deployed using ” private” (non WAN routed) IP address space IAW RFC 1918.

Note: This check does not apply to VoIP systems residing on the SIPRNet (i.e., VoSIP) and other closed globally addressed networks where it is the policy of the Program Manager to require individual “public” addresses to be individually assigned to each device connected to the network for the purpose of traceability and accountability. Therefore this is not a finding under these specific conditions.

The use of the term ” private” (non WAN routed) IP addresses in this sense means that the addresses are not routed or advertised across the internet by international agreement. NIPRNet also follows this policy. RFC 1918 addresses are routable within the LAN enclave. Deploying VoIP Systems on such an address space enhances security of the VoIP environment by denying access from outside routable addresses, thus effectively hiding the voice network. If VoIP systems are not deployed on ”private” address space and if the address space is not properly configured, managed, and controlled, the VoIP network could be accessed by unauthorized personnel resulting in security compromise of site information and resources.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.
RFC 1918 "Private" address ranges are defined as 10.0.0.0 - 10.255.255.255; 172.16.0.0 - 172.16.255.255; 192.168.0.0 - 192.168.255.255

Note: This check does not apply to VoIP systems residing on the SIPRNet (i.e., VoSIP) and other closed globally addressed networks where it is the policy of the Program Manager to require individual “public” addresses to be individually assigned to each device connected to the network for the purpose of traceability and accountability. Therefore this is not a finding under these specific conditions.

Fix(es): > Implement RFC 1918 addressing (Manual) > Use RFC 1918 addressing for all voice components. Monitor and control the use of this address space.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0082 V0008294 CAT II VoIP DHCP server NOT Dedicated

8500.2 IA Control: ECSC-1

Vulnerability A DHCP server used for IPT / VoIP terminal IP address assignment, is not dedicated to the IPT / VoIP system

Vulnerability Discussion: Requirement: The IAO will ensure that when using DHCP for address assignment, different servers are used for voice components and data components. Additionally, the IAO will ensure that these servers will reside in their respective voice or data address space.

When using Dynamic Host Configuration Protocol (DHCP) for address assignment, different servers will be used for voice components and data components. That is to say that a DHCP server serving VoIP devices needs to be in the VoIP domain i.e., same address space. This alleviates the need to route DHCP requests into the data environment on the LAN. The best practice is to manually assign addresses when authorizing the instrument by generating its configuration file.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Dedicate a VoIP DHCP Server (Manual) > If DHCP is used to initialize VoIP phones, Implement a dedicated DHCP server or manually assign addresses when authorizing the instrument by generating its configuration file.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0085 V0008295 CAT III VoSIP on SIPRNet NOT properly addressed

8500.2 IA Control: ECSC-1, DCPA-1

Vulnerability VoSIP systems and components residing on the SIPRNet ARE NOT utilizing address blocks assigned by the DRSN VoSIP PMO.

Vulnerability Discussion: Requirement: The IAO will ensure that all VoSIP systems and components residing on the SIPRNet utilize address blocks assigned by the DRSN VoSIP PMO.

IP addresses that are used by IPT / VoIP systems that are part of the VoSIP system using the SIPRNet as the VoSIP WAN, must be assigned from the pool of SIPRNet addresses that is maintained by the DRSN VoSIP PMO. This is to maintain the segregation of the Voice and data environments on the SIPRNet as required by this STIG. This also facilitates proper routing and flow control over the traffic between VoSIP addresses.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.1

Checks: > Review VoSIP address assignments (Manual) > Review address assignment documentation provided by the DRSN PMO- VoSIP department
> Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Obtain & use VoSIP addresses (Manual) > Obtain and assign IP addresses as provided by the DRSN PMO- VoSIP department

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0090 V0008350 CAT III NO firewall between voice and data VLANs & LCC

8500.2 IA Control: DCPA-1: ECSC-1

Vulnerability A stateful inspection firewall is not used between the voice and data VLANs and between the voice VLANs and the VoIP core control equipment on the network to protect VoIP system and communications.

Vulnerability Discussion: Requirement: The IAO will ensure that voice or data traffic between the data and voice VLANs and between the voice VLANs and the VoIP core control equipment is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.

Firewalls, routers, and switches must be implemented in a manner that will compartmentalize VoIP servers and communications from unauthorized access. This is necessary to limit and control (i.e., block) access from the data network to the IP telephony network. Such traffic must be blocked if there is no compelling need for it. Systems or devices that must be accessed from both the data and voice VLANs must be placed in a VLAN separate from both so that traffic to and from this VLAN is controlled and that there is no direct traffic between the voice and data VLANs. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. This firewall must control all traffic between the various VLANS discussed here.. This will mitigate possible malicious attacks that may originate from within the data network. At minimum IP filtering must be implemented between the IP telephony network and the IP data network.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.
> Locate/inspect the VoIP firewall (Manual) > Locate the firewall used to protect the VoIP system / portion of the network. Review current configuration files to confirm compliance

#########

Review current configuration: Review current configuration files of effected devices and confirm compliance

Fix(es): Implement proper VoIP firewall (Manual) > Implement a stateful inspection firewall between the IP telephony (VoIP) network and the IP data network. Additionally control traffic to and from the voip phone VLANs and the VoIP core equipment. (i.e., LCC, media gateways, messaging systems, etc).

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0095 V0008328 CAT II The Data Enclave Perimeter does not block VoIP

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability The data network perimeter protection is NOT configured to block all traffic destined to or sourced from the Voice VLAN IP Address space and VLANs

Vulnerability Discussion: Requirement: The IAO will ensure that the Data network perimeter protection (i.e., Data premise router, Data perimeter firewall) is configured to block all traffic destined to or sourced from the Voice VLAN IP Address space and/or fulfill one or more of the traffic control requirements noted above under VLAN traffic control.

Enclave boundary Firewalls and premise routers should be implemented in a manner that will protect the VoIP servers, VLANs, and communications from unauthorized access. This is necessary to limit and control access from the data network and from influences from outside the enclave to the IP telephony network. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. At minimum IP filtering should be implemented between the IP telephony network and the WAN as well as the IP data network. This will mitigate possible malicious attacks that may originate from within the data network. Additionally, this will force any approved WAN VoIP traffic to go through the VoIP firewall structure.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Block VoIP at data firewall (Manual) > Configure the enclave perimeter premise router and data firewall to block all traffic to and from the Voice VLANs and IP Address space. Additionally configure the Premise router to route approved VoIP traffic from the WAN to the VoIP firewall.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0100 V0008230 CAT II VoIP system is not in its own VLAN(s)

8500.2 IA Control: DCPA-1: ECSC-1

Vulnerability VoIP systems do not reside on dedicated and separate VLAN(s) from the data network.

Vulnerability Discussion: Requirement: The IAO will ensure that the local network supporting IPT implementations (i.e., the underlying data network) is configured using VLANs, and that at a minimum, one voice VLAN has been configured to segregate voice traffic from data traffic.

The implementation of VLAN technology serves to mitigate the risk that a DoS attack or packet sniffing, sourced from the data network. Will affect the voice network and vice versa. In addition, placing voice and data traffic into separate VLANs will reduce competition for the network and thus reduce latency (queue/wait time) for transmission services, which will reduce the possibility of denial of voice services. This also reduces the Ethernet broadcast domain thereby reducing network overhead. Since VoIP is very latency sensitive this segmentation approach is the most economical way to improve performance in an existing network infrastructure.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fix(es): Segregate VoIP systems - VLANs (Manual) > Deploy VoIP systems and components on a dedicated VLAN structure that is separate from the data network VLAN structure. A minimum of one VLAN is required. More than one is highly recommended.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0101 V0008296 CAT III Multiple IPT / VoIP VLANs not implemented

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability Multiple IPT / VoIP VLANs are not implemented

Vulnerability Discussion: Requirement: The IAO will ensure that the voice network is subdivided into multiple VLANs to segregate VoIP devices by type and function. At a minimum, this shall include five VLANs containing the following as might be applicable: call control servers, message servers (voice-mail, e-mail, unified), gateways, VoIP phones, and workstations with soft phones.
Suggested VLANs
- Call processing and voice DHCP servers
- Directory servers
- Message servers and/or servers that might be accessed from both the data network and the VoIP network.
- Gateways – possibly multiple VLANs for multiple types of gateways
- WAN Access firewalls

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Implement mult. VoIP VLANs (Manual) > Implement a multiple VLAN IPT / VoIP environment. Upgrade the network to support this if necessary.
> Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0102 V0008335 CAT II NO VLANs for Mutually accessible systems

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability Message servers or workstations with soft phones have not been placed in their own VLAN(s)

Vulnerability Discussion: Requirement: The IAO will ensure that servers or devices that are to be accessed from both the voice and data networks (i.e., message servers or workstations with soft phones) reside in their own protected VLANs. Mutually accessible servers may be placed in the DMZ of a dedicated stateful firewall placed between the voice and data networks per voice/data network protection requirements.

This practice enhances the segregation between the IPT / VoIP and data portions of the LAN by requiring that the traffic into and out of this VLAN be controlled by a layer 3 device that would not allow direct traffic across this VLAN between the IPT / VoIP and data portions of the LAN.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0103 V0008304 CAT II VLANs not Network STIG compliant

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability The IPT / VoIP VLANs are NOT configured according to the Network Infrastructure STIG.

Vulnerability Discussion: Requirement: The IAO will ensure that the local network’s VLANs are implemented in accordance with the VLAN section of the Network Infrastructure STIG.

See the Network Infrastructure STIG & Checklist for a discussion of the associated vulnerabilities.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing switch/router configuration files, that unused ports are disabled. Site personnel provide these files.
> Review DSN SRR results (Manual) > Review the results of the most recent Network SRR or Self Assessment. If there are a significant number of findings reported or if the Network Infrastructure STIG was not applied, this is a finding.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Upgrade/configure the LAN (Manual) > Upgrade the LAN infrastructure as necessary to meet Network Infrastructure and Enclave STIG requirements.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0105 V0008305 CAT II Devices NOT connected to proper VLAN

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability IPT / VoIP instruments and/or data workstations are NOT connected to the VLANs that are designated for their use.

Vulnerability Discussion: Requirement: The IAO will ensure that IP phones (that do not contain a multi-port switch), and servers providing voice services are connected to switchports with membership only to the voice VLAN(s). Additionally, the IAO will ensure that data workstations (without approved Soft Phones) are connected to switchports with membership only to the data VLAN(s).

These devices are to be connected to the VLANs that have been configured for their proper traffic control and protection of the Voice network.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance
> Inspect effected devices (Manual) > Inspect a sampling of effected devices to confirm compliance. Review device connections and port connections to determine if they are properly connected.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Comply with Policy - VLAN assignment (Manual) - Connect data devices such as workstations to the data VLANs only. Connect voice devices such as IPT/VoIP phones, media gateways, and LCCs to the appropriate Voice VLANs only.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0110 V0008306 CAT II IP Phone switches NOT disabled or NOT using 802.1Q

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability IP phones containing a multi-port switch do NOT utilize 802.1Q VLAN tagging and/or the PC port is not disabled.

Vulnerability Discussion: Requirement: The IAO will ensure that all IP phones containing a multi-port switch for connecting external devices such as a workstation, utilize 802.1Q trunking to separate voice and data traffic or have the data port(s) disabled.

Some IPT/VoIP instruments contain a multi-port switch for connecting external devices such as a workstation (i.e., PC port). These multi-port switches must be capable of supporting 802.1Q tagging for VLAN separation. If they do not, this will mix the voice and data networks if used.

Requirement: The IAO will ensure that all IP Phones and Soft Phones are:
- VLAN capable and that this function is enabled
- Assigned to the VoIP VLAN segment.

Many IP hardware phones provide a separate data port for the connection of a PC to the phone so that only a single cable is required to provide data and voice connectivity to the end users desktop. Additionally, some IP hardware phones are only capable of providing basic layer 2 connectivity, acting like a hub and combining the data and voice network segments. While other IP phones offer enhanced Layer 2 connectivity providing the option to use VLAN technology, to place the phone and the data traffic on two different VLANs. To ensure logical separation of voice and data in order to maintain the security of the VoIP environment, only layer 2 enhanced or VLAN capable phones should be considered for use.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing switch/router configuration files, that unused ports are disabled. Site personnel provide these files.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0111 V0008307 CAT II Access switches do not separate voice and data.

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability Access layer switch ports do not separate voice and data onto the appropriate voice and data VLANs that arrives from IP phones that contain a multi-port switch

Vulnerability Discussion: Requirement: The IAO will ensure that all access switch ports supporting IP phones that contain a multi-port switch route voice and data traffic to their respective VLANs.

Some IPT/VoIP instruments contain a multi-port switch for connecting external devices such as a workstation (i.e., PC port). These multi-port switches must be capable of supporting 802.1Q tagging for VLAN separation and the voice and data traffic must be tagged appropriately. If this feature is not supported, the access layer switch must detect the traffic types and rout the packets to the proper VLAN.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing switch/router configuration files, that unused ports are disabled. Site personnel provide these files.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0115 V0008323 CAT II IP filters between Voice and Data VLANs NOT used

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability IP filters have NOT been implemented between Voice and Data VLANs to control traffic such that it is restricted to planned traffic between authorized devices using approved ports, protocols, and services.

Vulnerability Discussion: Requirement: The IAO will ensure that traffic between all voice VLANs is filtered and controlled by a layer-3 switch/router ACL or a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services.

Firewalls, routers, and switches must be implemented in a manner that will compartmentalize VoIP servers and communications from unauthorized access. This is necessary to limit and control (i.e., block) access from the data network to the IP telephony network. Such traffic must be blocked if there is no compelling need for it. Systems or devices that must be accessed from both the data and voice VLANs must be placed in a VLAN separate from both so that traffic to and from this VLAN is controlled and that there is no direct traffic between the voice and data VLANs. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. This firewall must control all traffic between the various VLANS discussed here.. This will mitigate possible malicious attacks that may originate from within the data network. At minimum IP filtering must be implemented between the IP telephony network and the IP data network

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Implement Data-VoIP VLAN IP filtering (Manual) > Implement a stateful inspection firewall or router ACLs between the IP telephony (VoIP) network and the IP data network. Additionally control traffic to and from the VoIP phone VLANs and the VoIP core equipment. (i.e., LCC, media gateways, messaging systems, etc).

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0116 V0008325 CAT II Mutually accessible VLANs are not IP filtered

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability Traffic between the VLAN containing mutually accessible servers or devices (such as softphones) to and from the voice VLAN(s) or the data VLAN(s) is NOT filtered and controlled by a stateful inspection firewall.

Vulnerability Discussion: Requirement: The IAO will ensure that traffic between the VLAN containing mutually accessible servers or devices (such as softphones) to and from the voice VLAN(s) or the data VLAN(s) is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services. This firewall will block traffic between the voice and data VLANs or fulfill one or more of the traffic control requirements noted above.

Firewalls, routers, and switches should be implemented in a manner that will compartmentalize VoIP servers and communications from unauthorized access. This is necessary to limit and control access from the data network to the IP telephony network. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. At minimum IP filtering should be implemented between the IP telephony network and the IP data network. This will mitigate possible malicious attacks that may originate from within the data network.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Implement IP filtering - Mutual VLAN (Manual) > Implement IP filtering between the IP telephony (VoIP) network and the IP data network as well as to and from a VLAN housing mutually accessible systems or devices.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0120 V0008351 CAT III Unused voice VLAN ports are not disabled.

8500.2 IA Control: ECSC-1

Vulnerability Unused physical ports assigned to the voice VLAN are not disabled in access layer network switches.

Vulnerability Discussion: Requirement: The IAO will ensure that all unused ports are disabled and are placed in an unused VLAN.

Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that any unused physical access layer switch ports that could be assigned to the voice VLAN are disabled. If unauthorized personnel gains access to a VLAN through an unsecured physical switch port, they could cause disruptions, denial of service conditions, or access sensitive information. Disabling inactive or unused ports and assigning them to an unused VLAN prevents this type of unauthorized and unwanted activity.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.2

Checks: > Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing switch/router configuration files, that unused ports are disabled. Site personnel provide these files.
> Inspect effected devices (Manual) > Inspect a sampling of effected devices to confirm compliance. Plug a laptop or other Ethernet device into unused switch ports and see if link lights on both devices light indicating an active port.

Fix(es): > Disable unused VoIP ports (Manual)> Disable all unused physical network access ports or interfaces and assign them to an unused VLAN.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0122 V0008232 CAT III Unused data ports on IP phones are not disabled

8500.2 IA Control: ECSC-1

Vulnerability Data ports on IP phones are not being disabled or controlled as required.

Vulnerability Discussion: Requirement: The IAO will ensure that all IP phones with a multi-port switch have the data port disabled if a PC is not normally attached.

Many IP hardware phones provide a separate data port for the connection of a PC to the phone so that only a single cable is required to provide data and voice connectivity to the end users desktop. Additionally, some IP hardware phones are only capable of providing basic layer 2 connectivity, acting like a hub and combining the data and voice network segments. While other IP phones offer enhanced Layer 2 connectivity providing the option to use VLAN technology, to place the phone and the data traffic on two different VLANs. To ensure logical separation of voice and data in order to maintain the security of the VoIP environment, only layer 2 enhanced or VLAN capable phones should be considered for use.

Many attacks on DOD computer systems are launched from within the network by dissatisfied or disgruntled employees, therefore, it is imperative that any active IP Phone data ports be disabled. just as with unused physical ports on a network switch. If unauthorized personnel gain access to the VoIP or data environment through an unsecured data port, they could cause disruptions, denial of service conditions, or access sensitive information. Disabling data ports on IP Phones prevents this type of unauthorized and unwanted activity.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review phone configurations (Manual) > The reviewer must physically verify that unused ports are disabled by reviewing end instrument configuration files or screens. Site personnel demonstrate and/or provide accss to files and/or configuration screens.
> Inspect effected devices - phones (Manual) > Inspect a sampling of effected devices to confirm compliance. Plug a laptop or other Ethernet device into unused phone data ports and see if link lights on both devices light indicating an active port.

Fix(es): > Properly configure IP Phones (Manual) > Configure IP Phone workstation ports to be disabled unless their use is planned and authorized.
> Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0125 V0008308 CAT II Port security on voice VLAN NOT implemented

8500.2 IA Control: ECSC-1

Vulnerability Port security is NOT configured on all switchports with voice VLAN membership.

Vulnerability Discussion: Requirement: The IAO will ensure that port security is configured on all switchports with voice VLAN membership.

Many attacks on DOD computer systems are launched from within the network by dissatisfied or disgruntled employees, therefore, it is imperative that any active switchports with voice VLAN membership provide port security. If unauthorized personnel gain access to the VoIP VLAN through an unsecured switch port, they could cause disruptions, denial of service conditions, or access sensitive information. Port security on switchports with voice VLAN membership prevents this type of unauthorized and unwanted activity.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing switch/router configuration files, that unused ports are disabled. Site personnel provide these files.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Apply port security (Manual) > Apply port security to switchports with voice VLAN membership.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0127 V0008309 CAT II MAC addresses NOT limited on switchports

8500.2 IA Control: ECSC-1

Vulnerability The maximum number of MAC addresses that can be dynamically configured on a given switch port is NOT limited to that which is required to support authorized attached equipment (i.e., 1, 2, 3 or in some special cases 4).

Vulnerability Discussion: Requirement: The IAO will ensure that the maximum number of MAC addresses that can be dynamically configured on a given switch port is limited to that which is required to support authorized attached equipment (i.e., 1 – 3 or in some special cases 4).

Allowing too many MAC addresses on a switch port could allow a mini-hub or switch to be added to the voice VLAN port or PC/data port on a IP phone to which additional unauthorized devices or workstations to be connected. In the event that only a phone is to be attached with no PC connected to it, 1 or 2 MACs would be appropriate. If a PC is to be attached, then 3 is appropriate. In the special case where a security device is also attached to the phone along with a PC, then 4 would be appropriate.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.5.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing switch/router configuration files, that unused ports are disabled. Site personnel provide these files.
> Inspect effected devices (Manual) > Inspect a sampling of effected devices to confirm compliance

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Limit MAC Addresses (Manual) > Limit the maximum number of MAC addresses that can be dynamically configured on a given switch to that which is required (i.e., 1 – 3). IP phones with a multi-port switch (data/PC port) would require 3 MAC addresses if a PC is attached while only 2 if no PC is to be attached, IP phones without a multi-port switch (data/PC port) would only require 1 MAC address. In the special case where a security device is also attached to the phone along with a PC, then 4 would be appropriate.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0130 V0008318 CAT II Softphone are installed without DAA approval

8500.2 IA Control: ECSC-1

Vulnerability Softphone are installed and used without DAA approval

Vulnerability Discussion: Requirement: The IAO will ensure that written DAA approval is obtained prior to the use or installation of any IP Soft Phone agent software. The IAO will maintain documentation pertaining to such approval for inspection by auditors.

IP Soft Phone agents inherently reside in a data segment but require access to the voice network in order to access call control, place calls, and leave voice messages. Soft Phones are not as resistant to attack as hardware phones. Soft Phone hosts (desktop PCs) are more vulnerable to attacks due to the greater number of possible entries into the system. These entry mediums include the OS, resident applications, and enabled services all of which could be vulnerable to worms, viruses, etc. In addition, since the Soft Phone resides on a data segment, it is susceptible to any attack against that segment and not just the host itself. In contrast, IP hardware phones can reside in a protected VoIP segment and run proprietary OSs, and with limited network services enabled they are less likely to have vulnerabilities. Because the deployment of Soft Phones provides a conduit for malicious attack against the voice segment, these phones pose great risk to the VoIP environment.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.6

Checks: > Inspect effected devices (Manual) > Inspect a sampling of effected devices to confirm compliance
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.
> Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.

Fix(es): > Obtain DAA approval - Softphones (Manual) > Obtain DAA approval for softphone installation and use. Be sure the DAA is informed regarding the IA issues with using softphones. Maintain DAA approval documentation. Otherwise discontinue use and remove any installed softphones

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0135 V0008235 CAT III A local Soft Phone policy does not exist

8500.2 IA Control: DCSD-1, ECSC-1

Vulnerability A local policy does not exist prohibiting the use of personal installation and use of IP Soft Phone agents, etc.

Vulnerability Discussion: Requirement: The IAO will ensure a local IP Soft Phone policy exists and is being enforced that addresses the following:
- Prohibits the installation and use of IP Soft Phone agent software on workstations (fixed or portable) intended for day-to-day use in the users normal workspace.
- Prohibits the use of IP Soft Phone agent software in the users normal workspace, which has been approved and installed on a portable workstation for the purpose of VoIP communications while traveling.
- Prohibits the installation and use of IP Soft Phone agent software clients that are independently configured by end users for personal use or that is provided by commercial IPT service providers.
- Requires prior justification and DAA approval for the use of any IP Soft Phone agent software.
- Requires that the justification and DAA approval of IP Soft Phone agent software use is reviewed annually and approval renewed if justified.

Use of IP Soft Phone applications can introduce additional security vulnerabilities and considerations, which if left unmitigated, can expose government information systems to attack. All IP Soft Phone applications must be reviewed and kept to a minimum needed for operations. Reviewing IP Soft Phone applications requested and specifically approving for use only those needed for mission requirements will minimize risk for unauthorized access to DOD resources. The use of Soft phone agent software must be controlled and should be used only after the DAA is made aware of the security risk involved and approved their use. Any VoIP traffic to and from soft phone clients that have been independently installed and configured by an end user for personal use is prohibited within any DOD information systems. A local policy does not exist that prohibits the use of independently installed and configured Soft Phones.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.6

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fix(es): > Comply with Policy - Softphones (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy. Establish and enforce a policy to meet the requirements. Obtain DAA approvals as needed, periodically revalidate and update DAA approvals, perform periodic inspections and reviews.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0140 V0008319 CAT II Workstations with softphones NOT compliant

8500.2 IA Control: ECSC-1

Vulnerability Host systems (i.e., workstations), on which Soft Phones are installed, DO NOT comply with all applicable STIGs including but not limited to: OS, Application, Desktop Application.

Vulnerability Discussion: Requirement: The IAO will ensure that host systems (i.e., workstations), on which Soft Phones are installed, comply with all applicable STIGs including but not limited to: OS, Application, Desktop Application.

An un-STIGed workstation on the network places not only the workstation at risk for compormise but also places the entire network at risk. Too many vulnerabilities are addressed by the applicable STIGs to discuss here. Refer to the appropriate STIG(s) for details.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.6

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review Workstation SRR results (Manual) > Review the results of the most recent OS and Desktop SRR or Self Assessment of workstations containing softphones. If there are a significant number of findings reported or if the DSN STIG was not applied, this is a finding. Perform the necessary SRRs if necessary.

Fix(es): > STIG Workstations (Manual) > Properly configure all workstations per requirements in all applicable STIGs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0150 V0008233 CAT III PC-based soft-phones not properly implemented.

8500.2 IA Control: DCPA-1: ECSC-1

Vulnerability PC-based, software IP phones (soft phones) were found in use without a dedicated or 802.1Q capable network interface card (NIC) and VoIP VLAN.

Vulnerability Discussion: Requirement: The IAO will ensure that if/when approved Soft Phones are used in the LAN, the following conditions are met:
- The host computer contains a Network Interface Card (NIC), (commonly called a network adaptor) that is 802.1Q (VLAN tagging) and 802.1P (Priority tagging) capable.
- The host computer, NIC, and IP Soft Phone agent software is configured to use separate 802.1Q VLAN tags for voice and data.
- Alternately, dual NICs may be used where voice traffic is routed to one NIC and data traffic is routed to the other. Each NIC is connected to an access switch port residing in the appropriate VLAN.
- The host computer will be connected to separate voice and data VLANs that have been created expressly for the Soft Phone host(s). That is to say that the LAN should have a voice VLAN and a data VLAN dedicated to hosts with IP Soft Phone agents installed.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.6

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fix(es): > Install an appropriate NIC (Manual) > Install a separate dedicated NIC bound to the VoIP application, or an 802.1Q capable NIC. Assign the appropriate VLANs separating voice and data traffic.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0160 V0008236 CAT II Remote softphones are not properly implemented

8500.2 IA Control: ECSC-1

Vulnerability Remote softphones are not implemented according to requirements.

Vulnerability Discussion: Requirement: Requirement: The IAO will ensure that if/when approved Soft Phones are used in remote connectivity situations, the following conditions are met:
- The host computer connects to the “home enclave LAN” through an encrypted Virtual Private Network (VPN) connection.
- The VPN is terminated at the enclave boundary in accordance with the Enclave STIG
- The voice and data traffic is routed appropriately to separate voice and data VLANs in the “home LAN” through the appropriate voice and data firewalls
- The IP Soft Phone agent connects to the Local Call Manager Controller on the “home enclave LAN” through the VPN using “home enclave LAN” IP addressing.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.6

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Inspect effected devices (Manual) > Inspect a sampling of effected devices to confirm compliance
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0165 V0008321 CAT II Call center not configured as an enclave

8500.2 IA Control: ECSC-1; DCPA-1

Vulnerability A Call center is not configured as an enclave and secured in accordance with all applicable STIGs

Vulnerability Discussion: Requirement: The IAO will ensure that, if/when approved Soft Phones are used in a call center situation; the call center network is configured as a separate enclave and secured in accordance with all applicable STIGs.

A Call Center is a special telephony application. Usually its mission is of a critical nature. Downtime or attacks would be detrimental to the call center effectively fulfilling its mission. A Call Center should therefore be configured within its own network enclave to prevent or mitigate threats or attacks. This enclave should have a closed architecture or have appropriate firewalls at the boundary in compliance with all applicable STIGs. Additionally a Call Center may tightly integrated with data applications and or utilize softphones that make it impossible to maintain the separation of voice and data traffic as required for normal IPT/VoIP systems described elsewhere in this STIG. Such call centers should also be located in facilities that provide a heightened level of physical security (i.e., controlled access area). All requirements in this STIG regarding separation/segmentation of voice and data must be applied unless these measures break the call center application.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.6

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review network diagrams - Call Center (Manual) - Review network diagrams and device configurations as appropriate, to confirm that a call center is configured as an enclave.

Fix(es): > Comply with Policy (Manual)> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
> Upgrade/configure the LAN (Manual) > Upgrade the LAN infrastructure as necessary to comply with policy

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0180 V0008238 CAT II Stateful firewalls not used at VoIP/WAN boundary

8500.2 IA Control: EBBD-2, EBBD-3, ECSC-1

Vulnerability A Stateful inspection firewall has not been deployed at the VoIP LAN-to-WAN connection.

Vulnerability Discussion: Requirement: The IAO will ensure that VoIP aware firewalls are deployed at all approved VoIP enclave to WAN connections providing VoIP call connectivity. Such firewalls must employ stateful packet inspection and dynamic port mapping.

LAN-to-WAN VoIP connections may have application filtering issues when using the H.323 protocol. This problem is encountered when return TCP connections on higher range ports attempt to establish. There are similar issues when using SIP signaling. Therefore, VoIP aware stateful firewalls must be used at LAN-to-WAN VoIP call connection network points to protect the internal VoIP environment.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Locate/inspect the VoIP firewall (Manual) > Review network diagrams and confirm firewall type and deployment location within the VoIP environment. Review firewall configuration for H.323 and SIP rule settings.

Fix(es): Implement proper VoIP/WAN firewall (Manual) > Implement stateful inspection firewalls at VoIP LAN-to-WAN connection points. And apply proper rule sets.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0190 V0008331 CAT II NAT is NOT used on VoIP WAN connections.

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability NAT is NOT used on VoIP WAN connections.

Vulnerability Discussion: Requirement: The IAO will ensure that NAT is implemented on approved VoIP enclave to WAN connections.

To maintain the private addressing scheme (RFC 1918) on in the VoIP LAN enclave, Network Address Translation (NAT) must be implemented at the VoIP enclave WAN connection point. This provides additional protection in that hackers outside the VoIP network segment will not be able to scan the VoIP segment for vulnerabilities.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Implement VoIP NAT (Manual) > Implement NAT on the VoIP enclave firewall.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0200 V0008240 CAT III Voice Perimeter firewalls are not dedicated

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3,

Vulnerability Voice enclave Perimeter firewalls are not dedicated to VoIP connections.

Vulnerability Discussion: Requirement: The IAO will ensure all voice enclave security perimeter firewalls are dedicated to VoIP

The IAO will ensure all VoIP security perimeter firewalls are dedicated to VoIP traffic to reduce transmission latency caused by access control list (ACL) processing.

Firewalls, routers, and switches should be implemented in a manner that will compartmentalize the VoIP servers and phones from unauthorized access. This is necessary to limit and control access from the data network and WAN to the IP telephony network, firewall controls are to be placed in front of all networks and components supporting VoIP servers. VoIP systems require many ports to be opened in firewalls to avoid a noticeable delivery delay. The protocol used for carrying VoIP traffic through the network uses a wide range of ports (10024 to 65535) to transport packets. The filtering of VoIP packets is difficult to perform to avoid noticeable delivery delay. It is for this reason that firewalls are to be dedicated to the VoIP environment to adequately handle telephony traffic. This will also help to mitigate the risk of possible malicious attacks that may originate from within the data network.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.2

Checks: > Review Network Diagrams- Firewall (Manual)> Review network diagrams and confirm firewall type and deployment location within the VoIP environment. Ensure firewalls are dedicated to processing VoIP traffic.

Fix(es): > Dedicate VoIP firewalls (Manual) > dedicate firewall and filtering device to the VoIP environment.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0210 V0008241 CAT II VoIP firewall management traffic is not controlled

8500.2 IA Control: EBRP-1: EBRU-1: ECCT-1: ECNK-1: ECSC-1,
EBBD-1, EBBD-, EBBD-3

Vulnerability VoIP firewall administrative/management traffic (i.e. ports 69,161,162, 389) is not being controlled or encrypted at the VoIP network perimeter.

Vulnerability Discussion: Requirement: The IAO will ensure VoIP perimeter firewall administrative/management traffic is blocked at the perimeter or tunneled/encrypted using VPN technology at the security perimeter (ports 69, 161, 162, 389).

Administrative and management access to firewalls supporting the VoIP environment for configuration management must be protected. To securely protect the telephony network, firewall access must be controlled to guard against unauthorized intrusion, which could result in system or network compromise. Administering or managing firewalls from the same network used for public use increases the risk of compromising data that will allow unauthorized people access to critical areas of the VoIP network. At a minimum, these types of sessions must be controlled by port and IP or encrypted at the enclave perimeter.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.9.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations - firewall (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.
#########

Review current configuration: Review current configuration files of effected devices and confirm compliance

Fix(es): > Control firewall admin traffic (manual) > Control all VoIP firewall administrative/management traffic by IP port and IP address if traffic internal to the enclave. If remote connections are required from outside the enclave use encryption to secure the connections in addition to filtering by IP port and IP address.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0220 V0008242 CAT II MS-SQL port 1433 not controlled at VoIP boundary

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability MS-SQL port 1433 is not being controlled at the VoIP security perimeter.

Vulnerability Discussion: Requirement: The IAO will ensure MS-SQL (port 1433) is blocked at the VoIP security perimeter.

Microsoft SQL Server (MS-SQL) is used by some VoIP solutions and MS-SQL Server traffic uses port 1433. There are several serious vulnerabilities associated with MS-SQL Server that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts. MS-SQL vulnerabilities are well publicized and actively under attack. In order to ensure the security of VoIP environment this port must be controlled if not blocked at the enclave perimeter.

References: nternet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations - firewall (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

Fix(es): > Block MS-SQL port 1433 (manual) > Block MS-SQL port 1433 at the VoIP security perimeter.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0230 V0008243 CAT III NTP port 123 not controlled at VoIP boundary

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability The network time protocol (NTP) port 123 is not blocked at the VoIP security perimeter and clock is not being derived from a local global position system (GPS).

Vulnerability Discussion: Updated Requirement: The IAO will ensure the network time protocol (NTP port 123) is blocked at the VoIP-WAN security perimeter. The IAO will ensure the internal VoIP network device time is derived from the premise router of the LAN on which the VoIP system resides. The premise router is synchronized with two up-stream NTP servers and acts as the NTP server for the LAN. This is in accordance with the Network Infrastructure STIG and is for the purpose of logging and audit time stamp coordination with other devices and systems on the LAN. This includes the IP network side of media gateways (and other TDM-IP devices) but not the TDM side of the device.

VoIP network administrative/audit time should be derived from the local network premise router.
The Premise router should syncronise its time from 2 of the Naval Observatory Tier1 NTP servers.

Timing and synchronization is critical to the telephony network since VoIP packets cannot be re-transmitted to compensate for unstable or intermittent timing. Network Time Protocol (NTP) is used administratively to automatically synchronize computer clock times among systems on a network. Critical VoIP severs depend on an NTP server by which to synchronize their own clocks. In order to ensure proper synchronization with other VoIP components NTP must be derived from GPS system. This is especially important when making VoIP calls across domains in order to ensure global synchronization.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations - firewall (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

Fix(es): > Block (NTP) port 123 (manual) > Block (NTP) port 123 at the VoIP-WAN security perimeter.
> Derive time locally (Manual) > Derive VoIP network administrative/audit time from the local network premise router.
>Syncronise Premise router time (Manual) > Syncronise Premise router time to 2 of the Naval Observatory NTP servers in accordance with the Network Infrastructure STIG

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0240 V0008244 CAT II Terminal services (port 3389) is not being blocked

8500.2 IA Control: EBRU-1, ECCT-1, ECNK-1, ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability Terminal services (port 3389) is not being blocked, or if used, encrypted at the VoIP security perimeter.

Vulnerability Discussion: Requirement: The IAO will ensure Terminal Services or remote desktop protocol (port 3389) is blocked at the security perimeter or that these connections are encrypted.

Terminal Services enables users to log on to a remote system as if they were logging on locally. The Terminal Services client program, which runs on any version of Windows, redirects the local keyboard and mouse and emulates the remote video display. Some VoIP venders use terminal services to remotely manage their VoIP systems. If Terminal Services access is compromised the whole VoIP environment would be in jeopardy and at risk of compromise or even denial of service. It is imperative that all Terminal Services connections be blocked at the enclave boundary and if used all connections are to be encrypted.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations - firewall (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

Fix(es): > Block Terminal Services (Manual)> If not required, block all Terminal Services access (port 3389) at the security enclave boundary. If Terminal Services is required, encrypt all connections at the security enclave boundary.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0245 V0008245 CAT II Remote firewall Web connections are not proxied

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability Remote firewall Web connections for firewall administration are not proxied at the site perimeter.

Vulnerability Discussion: Requirement: The IAO will ensure that all remote HTTP access to the VoIP enclave perimeter firewalls is proxied. HTTP access from the VoIP enclave, if required, should route through the data enclave. Additionally HTTPS should be used in place of this if possible.

This includes ports 80, 8080, 443, 8002, and 8003.

In order to ensure the security of VoIP perimeter firewalls it is imperative that administrative/management connections and access to the devices be controlled. Some VoIP systems support web-based remote administration using the HTTP protocol. Web access is a viable mechanism for monitoring, configuring, and attacking critical devices such as firewalls. It is imperative that remote Web access for administrative purposes be proxied at the enclave perimeter.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.2

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations - firewall (Manual) > Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

Fix(es): > Proxy "Web based" Management (Manual) > Proxy all remote firewall and VoIP system "web basd" administrative connections at the enclave perimeter.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0270 V0008247 CAT II Critical servers supporting VoIP are not dedicated

8500.2 IA Control:	ECSC-1
Vulnerability	Critical servers supporting the VoIP telephony environment are not dedicated to VoIP telephony applications.
Vulnerability Discussion:	Requirement: The IAO will ensure that VoIP servers are dedicated to only applications required for VoIP operations. VoIP servers represent mission critical equipment that contain potentially sensitive information that needs to be secured and treated with the same precautions as any other servers containing sensitive information. Dedicating critical VoIP servers to only VoIP required applications is key to securing the IP telephony environment. To minimize possible risk these servers are to be dedicated to the IP Telephony applications required for VoIP operations minimizing the chance of infection or attack through an unused, unnecessary application residing on the system.
References:	Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.1
Checks:	> Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable. > Review Server applications (Manual) > Review the server for additional applications not required for VoIP operational support. ######### Inspect servers for extra apps: Inspect the servers for applications that are not related to the primary function / purpose of the server
Fix(es):	> Dedicate VoIP Servers (Manual)> Dedicate critical servers supporting the VoIP telephony environment to running VoIP telephony applications only. Additionally, remove all unnecessary portions of the Operating System such as sub-applications or files and routines that are not required to support the VoIP telephony system.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0280 V0008248 CAT III Servers supporting VoIP are not STIG compliant

8500.2 IA Control:	ECSC-1
Vulnerability	Critical servers supporting the telephony environment have not been secured in compliance with applicable STIG guidelines.
Vulnerability Discussion:	Requirement: The IAO will ensure that critical VoIP servers have been secured in compliance with all applicable STIGs (i.e., UNIX, Microsoft NT/Win2K, database, web, etc.). VoIP servers represent mission critical equipment that contain potentially sensitive information that needs to be secured and treated with the same precautions as any other server containing sensitive information. Securing critical VoIP servers is key in securing the IP Telephony environment. Some vendors provide IP Telephony services on their own proprietary systems while others provided these services on standard UNIX and Microsoft Windows based systems. Most known vulnerabilities exist on UNIX and Windows based operating systems. They may also use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Additionally, application security guidance may be applicable for the vendor's application that makes the server or device perform the functions, or the management, of the system. Therefore, the securing of these voice processing and signaling platforms, to include their installed applications, is vital in protecting the VoIP environment from malicious attack. The specific VoIP system server or device determines the applicability of any given STIG.
References:	Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.1 DODI 8500.2 security control - ECSC-1
Checks:	> Review server SRR results (Manual) > Obtain a copy of all applicable SRR or Self Assessment results and review for compliance. If there are a significant number of findings reported or if the an applicable STIG was not applied, this is a finding. If SRR results are not available, then perform all applicable SRRs on a representative number of VoIP system servers and devices. Note: The specific VoIP system server or device determines the applicability of any given STIG. Many VoIP system servers or devices are based on general-purpose operating system such as Microsoft Windows, Unix, or Linux. They may use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Determine what the system under review is based upon and perform the associated SRRs. Additionally, an application SRR may be applicable for the vendor's application that makes the server or device perform the functions or the management of the system.
Fix(es):	> Secure critical servers (Manual) > Secure critical servers supporting the telephony environment. Apply all applicable STIGs (i.e. UNIX, Microsoft Windows, database, web, etc. UNIX, Win2k/NT, DSN, etc.) and ensure compliance with applicable STIG guidelines.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0281 V0008349 CAT II Not using Vendor originated Patches

8500.2 IA Control:	ECSC-1
Vulnerability	Software patches for critical VoIP servers and other IPT devices DO NOT originate from the system manufacturer and are NOT applied in accordance with manufacturer’s instructions.
Vulnerability Discussion:	Requirement: The IAO will ensure that software patches for critical VoIP servers and other IPT devices originate from the system manufacturer and are applied in accordance with manufacturer’s instructions. Many IPT / VoIP systems are based on general-purpose operating systems and applications such as databases and web servers (i.e., Windows XX, MS-SQL, IIS, Unix, LINUX, etc). The original vendors of these general-purpose software packages provide patches for their individual packages. A vendor of a IPT / VoIP system must test and approve these patches for use on their system before they are applied in the event that the OEM patch might break a portion of the IPT / VoIP system or degrade it’s security. The IPT / VoIP vendor may have to modify the OEM patch before releasing it to their customers.
References:	Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.1.1
Checks:	> Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.
Fix(es):	> Only Apply vendor approved patches (Manual) – Only Apply vendor-approved or vendor supplied patches. Correct site policy to require only vendor provided and approved patches are applied.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0282 V0008286 CAT II Not applying Vendor approved IAVA Patches

8500.2 IA Control: ECSC-1

Vulnerability IAVAs are NOT being referred to IPT / VoIP vendors for approval and patch distribution

Vulnerability Discussion: Requirement: The IAO will ensure that all IAVAs applicable to the general-purpose systems and applications used in VoIP systems are referred to the system manufacturer for approval and patch distribution in order to maintain timely IAVA compliance.

IPT / VoIP vendors must be immediately advised of IAVAs that apply to their systems so that they can test the required patch / mitigation and subsequently distribute an approved patch for their system (in accordance with VoIP0281) so that the site can maintain IAVA compliance.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.1.1

Checks: Determine IAVA response (Interview) - Interview the IAO and/or SA to determine their response to IAVAs affecting the platforms supporting IPT / VoIP systems. Review patching records.

Fix(es): Comply with IAVA policy (Manual) – Comply with policy. Contact the VoIP system vendor upon receipt of a IAVA to determine if the vendor can provide the required approved patch or refer th IAVA to the vendor for testing and approval

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0290 V0008249 CAT II Remote admin of VoIP servers is not encrypted

8500.2 IA Control: EBRU-1: ECCT-1: ECNK-1: ECSC-1

Vulnerability Remote administrative connections to critical VoIP servers are not encrypted.

Vulnerability Discussion: Requirement: The system administrator will ensure all remote administrative connections to critical VoIP servers are encrypted.

In order to ensure the security of critical VoIP servers it is necessary that administrative connections be encrypted. Remote access connections are a viable mechanism for monitoring, configuring, and attacking these critical systems. It is imperative, that at a minimum, remote access connections to critical VoIP servers be encrypted at the enclave perimeter.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.9.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review Network Diagrams - remote access (Manual) > Review network diagrams and confirm network perimeter device configuration rule settings for specific port and proxy control.
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate a remote connection to a critical VoIP server and confirm encryption.

#########

Review current configuration: Review current configuration files of effected devices and confirm compliance

#########

Demonstrate Compliance: Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

Fix(es): > Encrypt all administrative access (Manual) > Encrypt all administrative access connections to critical VoIP servers. At a minimum these remote connections are to be encrypted at the enclave perimeter.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0295 V0008332 CAT II VoIP system management is not per DSN STIG

8500.2 IA Control: ECSC-1

Vulnerability The VoIP system management is not performed in accordance with the requirements in the DSN STIG

Vulnerability Discussion: Requirement: The IAO will ensure that all VoIP systems are managed in accordance with all requirements in the DSN STIG.

VoIP system management is not detained in the IPT/VoIP STIG. This version of the STIG refers to the DSN STIG for system management requirements.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.9

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices and confirm compliance
> Review network diagrams (Manual) > Review network diagrams and confirm VoIP system Management connections are encrypted.

Fix(es): > Comply with Policy (Manual)>- Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0300 V0008250 CAT II VoIP is not encrypted over a “public” IP WAN

8500.2 IA Control: EBRU-1: ECCT-1: ECNK-1: ECSC-1

Vulnerability VoIP traffic is being sent over a public IP network (i.e. internet, NIPRNet) without being encrypted.

Vulnerability Discussion: Requirement: The IAO will ensure that all VoIP traffic that is sent over approved VoIP enclave-to-WAN connections via an IP WAN network (i.e., Internet, NIPRNet,) is encrypted, at a minimum, between enclaves across the WAN.
NOTE: The inherent site-to-site encryption employed in classified networks, such as the SIPRNet, meets this requirement.

When WAN VoIP connections are established, all call privacy can be lost. Just as all DSN trunks are encrypted ensuring the privacy of subscriber calls any Wan-to-Wan VoIP call connection must be encrypted in order to maintain the same level of security. If Wan-to-Wan VoIP traffic is passed in the clear it is open to sniffing attacks. Encryption can be accomplished at the link-level through the incorporation of VPN technology. Gateway devices are normally designed to handle heavier processing loads and are also capable of providing link encryption. If implemented, either method would be transparent to the subscriber community but provide the same level of security and privacy that is provided to long distance voice calls processed by the DSN.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.8

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review network diagrams - Wan Connections (Manual) > Review network diagrams and device configurations as appropriate, to confirm VoIP LAN-to-Wan connections are encrypted.

#########

Review current configuration: Review current configuration files of effected devices and confirm compliance

Fix(es): > Encrypt VoIP LAN-to-Wan calls (Manual) > Secure all VoIP LAN-to-Wan call connections via encryption.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0310 V0008251 CAT II Legacy Unified mail, text to speech is enabled

8500.2 IA Control: ECSC-1

Vulnerability The unified mail, text to speech feature is enabled using an existing email system.

Vulnerability Discussion: Requirement: The IAO will ensure text-to-speech is disabled if the voice mail platform is configured to interact with a legacy corporate email system and both systems are not collocated in the same or adjoining VLANs as required under the VLAN section above.

Voice mail services in a VoIP environment are available in several different configurations. A legacy voice mail platform can connect to a VoIP environment to provide voice mail services for VoIP users. In the same respect, a VoIP voice mail platform can provide voice mail services to the legacy voice users and the VoIP users. Some VoIP voice mail systems are also capable of providing unified mail, by interacting with existing email messaging systems. If the legacy corporate email system is accessible to the VoIP system not placed in a VLAN that is separate from the data network VLANs, the text to speech feature wil degrade the separation of the voice and data environments and VLANs. See VLAN requirements above.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.10

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Demonstrate Compliance (Interview) > Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fix(es): > Disable unified mail text to speech (Manual) > Disable the text to speech of unified mail systems if using an existing/legacy email system for voice mail.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0330 V0008253 CAT II Voice mail system VoIP is not STIG compliant

8500.2 IA Control: ECSC-1

Vulnerability The Voice mail system supporting VoIP is not secured to applicable STIG guidance.

Vulnerability Discussion: Requirement: The IAO will ensure the server hosting the Voice Mail Service is properly secured in accordance with all applicable STIGs (i.e., Windows, Unix, Database, and Web).

Various VoIP solutions provide voice mail services support in different ways to include integrating these services with existing email services. When voice mail is leveraged off of an existing email server it leaves the telephony environment open to all vulnerabilities that exist on the data network. Many of these voice mail services can provide access to the VoIP environment via unsecured channels if servers are not secured. This can happen through the abuse and use of enabled but unused services or through known un-patched vulnerabilities that exist on common mail servers. To protect against this, all unused services are to be disabled and all voice mail application servers are to be secured using the applicable STIG guidance.

References: Voice over Internet Protocol (VoIP) STIG V1R1

Checks: > Review server SRR results (Manual) > Obtain a copy of all applicable SRR or Self Assessment results and review for compliance. If there are a significant number of findings reported or if the an applicable STIG was not applied, this is a finding. If SRR results are not available, then perform all applicable SRRs on a representative number of VoIP system servers and devices. Note: The specific VoIP system server or device determines the applicability of any given STIG. Many VoIP system servers or devices are based on general-purpose operating system such as Microsoft Windows, Unix, or Linux. They may use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Determine what the system under review is based upon and perform the associated SRRs. Additionally, an application SRR may be applicable for the vendor's application that makes the server or device perform the functions or the management of the system.

Fix(es): > Secure critical servers (Manual) > Secure critical servers supporting the telephony environment. Apply all applicable STIGs (i.e. UNIX, Microsoft Windows, database, web, etc. UNIX, Win2k/NT, DSN, etc.) and ensure compliance with applicable STIG guidelines.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0340 V0008254 CAT II Supporting application services not STIG Compliant

8500.2 IA Control: ECSC-1

Vulnerability Application services (i.e. SQL, IIS, Apache, Oracle, etc.) supporting the VoIP environment have not been secured to applicable STIG guidance.

Vulnerability Discussion: Requirement: The IAO will ensure the application services (SQL, IIS, Apache, Oracle, etc.) supporting the voice mail service are properly secured according to the appropriate STIGs.

Various VoIP solutions use various application services to provide Voice and voice mail support. Many of these applications can provide access to the VoIP environment via unsecured channels. This can happen through the abuse and use of enabled but unused services or through known un-patched vulnerabilities that exist on common application servers. All unused services are to be disabled and all application servers are to be secured using the applicable STIG guidance.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.10

Checks: > Review server SRR results (Manual) > Obtain a copy of all applicable SRR or Self Assessment results and review for compliance. If there are a significant number of findings reported or if the an applicable STIG was not applied, this is a finding. If SRR results are not available, then perform all applicable SRRs on a representative number of VoIP system servers and devices. Note: The specific VoIP system server or device determines the applicability of any given STIG. Many VoIP system servers or devices are based on general-purpose operating system such as Microsoft Windows, Unix, or Linux. They may use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Determine what the system under review is based upon and perform the associated SRRs. Additionally, an application SRR may be applicable for the vendor's application that makes the server or device perform the functions or the management of the system.

Fix(es): > Secure critical servers (Manual) > Secure critical servers supporting the telephony environment. Apply all applicable STIGs (i.e. UNIX, Microsoft Windows, database, web, etc. UNIX, Win2k/NT, DSN, etc.) and ensure compliance with applicable STIG guidelines.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0350 V0008255 CAT II Voice mail settings can be changed - unsecured

8500.2 IA Control: EBRU-1: ECCT-1: ECNK-1: ECSC-1

Vulnerability Voice mail settings can be changed by the subscriber via a unsecured/unencrypted connection.

Vulnerability Discussion: Requirement: The IAO will ensure the subscriber can only change their voice mail settings via the phone interface or through an SSL connection. HTTP and Telnet services will be disabled on the voice mail platform.

Access to voice mail services via an encrypted IP connection is inherently dangerous because anyone with a sniffer and access to the right LAN segment can acquire the subscribers account and password information. With this intercepted information a hacker could gain access to the subscribers voice mail, intercept sensitive information, and/or perform other destructive actions. It is for this reason that all subscriber connections to voice mail settings are to be encrypted using SSL, SSH, or other encryption if natively provided by the voice mail/VoIP system.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.10

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Demonstrate Voice mail Config. Process (Interview) > Have the IAO or SA demonstrate compliance with the requirement; Have the SA demonstrate from an IP Phone. If settings can also be changed via a web connection, ensure this connection utilizes SSL.

Fix(es): > Secure voice mail user config access (Manual) > Secure all subscriber access to voice mail settings with SSL, SSH or available encryption.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0360 V0008256 CAT II Wireless VoIP is being used without Wireless STIG

8500.2 IA Control: ECSC-1: ECWN-1

Vulnerability Wireless VoIP is being used without Wireless STIG security guidance applied.

Vulnerability Discussion: Requirement: The IAO will ensure that if wireless VoIP is used, the requirements contained in the Wireless STIG have been applied to the wireless VoIP environment.

The Incorporation of Wireless technology elevates many existing VoIP concerns such as quality of service (QoS), network capacity, provisioning, architecture and not the least important, security. Many government entities are exploring mobile communication solutions that include wireless VoIP that can meet critical needs for interoperability and flexibility. If this technology is deployed all the requirements in the VoIP STIG as well as those contained in the Wireless STIG are to be applied to the wireless VoIP environment.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.11

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.
> Review Wireless SRR results (Manual) > Review the results of the most recent Wireless Reviews and/or wireless discovery. IfWireless VoIP is used, and there are a significant number of findings reported against the WLAN or if the STIG was not applied, this is a finding.

Fix(es): > Comply with Wireless Policy (Manual) > (Manual) - Apply requirements contained in both the VoIP STIG and the Wireless STIG wherever VoIP over Wireless is used.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0361 V0008333 CAT II NO DAA approval for Wireless VoIP

8500.2 IA Control: ECSC-1, ECWN-1

Vulnerability Wireless VoIP is being used without DAA approval

Vulnerability Discussion: Requirement: The IAO will ensure that written DAA approval is obtained prior to the implementation of VoIP over WLAN. The IAO will maintain documentation pertaining to such approval for inspection by auditors.

The Incorporation of Wireless technology elevates many existing VoIP concerns such as quality of service (QoS), network capacity, provisioning, architecture and not the least important, security. Many government entities are exploring mobile communication solutions that include wireless VoIP that can meet critical needs for interoperability and flexibility. If this technology is deployed the DAA must be aware and accept the risk.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.11

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, Configuration files, DAA approvals, etc as applicable.

Fix(es): > Comply with Policy (Manual) > Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes:

VoIP 0370 V0008257 CAT II The VoIP system is not DSN APL certified

8500.2 IA Control: EBCR-1: ECSC-1

Vulnerability VoIP systems or networks are connected to the DSN or PSTN switching system without being certified and placed on the DSN APL.

Vulnerability Discussion: Requirement: The IAO will ensure that no VoIP systems or networks are connected to the DSN switching system without being certified, accredited, and placed on the DSN Approved Products List per DODI 8100.3.

Any VoIP network connected to any DSN switch poses a potential security risk to the network and should not be connected until Interroperability certification by the DISA Joint Interoperability Test Command (JITC) and Information Assurance Certivication and Accreditation by the DISN Security accreditation Working Group (DSAWG) is completed.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.13
Defense Switched Network (DSN) STIG V2R1 Section 6.0
Department of Defense Instruction (DODI) 8100.3, DoD Voice Networks, 16 January, 2004
Chairman Joint Chiefs of Staff Instruction (CJCSI) 6215.01b 23 SEP 2001 6A Para 12.
Public Law 107-314 2 December, 2002 , sections 352 and 353

Checks: > Confirm DSN APL Listing (Manual) > Verify that the VoIP system is listed on the DSN APL by checking at the following link: http://jitc.fhu.disa.mil/tssi/apl.html . If not, verify connection to the DSN. Attempt to make a call from an IP phone to a standard DSN phone. If this can be done, this is a finding.

Fix(es): > Comply with Policy - DSN APL (Manual) > Ensure non certified VoIP systems are not connected to the DSN. Sponsor the system for DSN APL testing and certification.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes: □

VoIP 0900 V0008329 CAT II External VoIP calls NOT routed via Media Gateway

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability Calls to and from the enclave system to external networks are NOT routed via Media Gateway

Vulnerability Discussion: Requirement: The IAO will ensure that all calls into and out of the VoIP network enclave are routed via a media gateway to the traditional TDM networks i.e., DSN and/or PSTN. An exception is made for DAA approved remote VoIP instruments and Soft Phones that connect to the VoIP network enclave via a VPN and are therefore part of the VoIP network.

As of the writing of the IPT/VoIP STIG V2R1, off-site VoIP Trunking is not approved for use in unclassified DOD telecommunications systems. The DOD DSN PMO is only certifying VoIP systems at the PBX-1, PBX-2, and SMEO level, as specified in the GSCR, for inclusion on the DSN APL. These systems are specified for use at the BPCS level. No systems are being certified to use VoIP Trunking for off-premise connections. Due to the fact that DOD policy requires that only DSN APL certified systems be deployed, IP trunking is not approved. All trunking connections to DOD VoIP networks must be through media gateways to the TDM DSN/PSTN.

This requirement is intended to assure proper access the DSN/PSTN as well as interoperability between VoIP systems in other enclaves that may be from different vendors. The Standard VoIP signaling protocols (SIP and H.323) were developed to provide signaling methods for the transport of voice and video across the Internet as well as some other types of Internet communications. As such, they were not developed to support the many features that we have come to rely on in today's TDM based enterprise phone systems. To overcome this lack of standardized features, each vendor of a VoIP system has developed their systems to provide these features in different ways. Some use modifications or extensions of the standard protocols, while others use proprietary protocols. Typically, these systems do not interoperate. Additionally, this supports current data firewall policy.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Implement Media Gateway (Manual) > Block all VoIP traffic at the enclave boundary and implement a media gateway to handle calls into and out of the enclave.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes: □

VoIP 0901 V0008330 CAT III VoIP trunking is used without DAA approval.

8500.2 IA Control: ECSC-1, EBBD-1, EBBD-, EBBD-3

Vulnerability VoIP trunking is used without DAA approval.

Vulnerability Discussion: Requirement: The IAO will ensure that written DAA approval is obtained prior to the implementation of IP Trunking connections from the VoIP enclave to the WAN. The IAO will maintain documentation pertaining to such approval for inspection by auditors

The use of VoIP Trunking can subject the enclave to threats from the WAN if the enclave boundary is not properly protected. VoIP communications requires that there be up to 4 ports opened in the boundary firewall for each call in progress. This can leave gaping holes in a enclave’s boundary.

References: Internet Protocol Telephony (IPT) & Voice Over Internet Protocol (VoIP) STIG V2R1 Section 3.7.2.1

Checks: > Interview the IAO and/or SA (Interview) > Interview the IAO and/or SA to confirm compliance through discussion, review of site policy, diagrams, documentation, configuration files, DAA approvals, etc as applicable.
> Review current configurations (Manual) > Review current configuration files of effected devices to confirm compliance

Fix(es): > Implement Media Gateway (Manual) > Block all VoIP traffic at the enclave boundary and implement a media gateway to handle calls into and out of the enclave.
> Obtain DAA approval - VoIP Trunking (Manual) > Obtain DAA approval for VoIP Trunking and use. Be sure the DAA is informed regarding the IA issues with using VoIP Trunking. Maintain DAA approval documentation. Otherwise discontinue use of VoIP Trunking.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:**

Notes: